CYBERCRIME INVESTIGATION HANDBOOK FOR POLICE OFFICERS

(5-DAYS PROGRAM)

सत्यमेव जयते

Ministry of Home affairs

Contents

Document Control ..... Error! Bookmark not defined.
CHAPTER 1 ..... **9**
Introduction to Cyber crimes **10**
Types of Cybercrimes **11**
1.1. Email related crime **11**
1.1.1. Email spoofing **11**
1.1.2. Phishing/vishing **11**
1.1.3. Email bombing **11**
1.1.4. Spamming **11**
1.1.5. Spear phishing **11**
1.2. Illegal Online transaction **12**
1.3. Job Frauds **12**
1.4. Cyber defamation **13**
1.5. Ponzi scheme **13**
1.6. Cyber stalking **13**
1.7. Cyber bullying **13**
1.8. Cyber pornography **13**
1.9. Cybercrimes/Attacks of advanced types **13**
1.10. Hacking **14**
1.11. Virus **14**
1.12. Worm **14**
1.13. Trojan **14**
1.14. Website defacement **14**
1.15. Salami Attack **14**
1.16. Cross-site scripting **14**
1.17. Web Jacking **15**
1.18. DOS/DDOS attacks **15**
1.19. Ransomware **15**
1.20. Data hiding technique **15**
1.20.1. Steganography **15**
1.21.1. Deep Web & Dark Web **16**
1.21.2. Cryptocurrency **17**
User awareness – Safe practices to mitigate cybercrimes **17**
CHAPTER 2 ..... **18**
Computer Networks, E-mails & Web Hosting **19**
Why should you read this Chapter? **19**
2. Introduction to computer networks **19**

2.1.1. Networking Requirements 19
2.1.2. Connection method 20
2.1.3. Wired technologies 20
2.2. Types of networks based on the physical scope 21
2.2.1. Personal Area Network 21
2.2.2. Local Area Network 21
2.2.3. Campus Network 21
2.2.4. Metropolitan Area Network 21
2.2.5. Wide Area Network 21
2.2.6. Virtual Private Network 21
2.2.7. Peer-to-peer (P2P) 22
Client-Server Architecture 22
2.3. The concept of IP address 22
2.3.1. Static IP Addresses 23
2.3.2. Dynamic IP Addresses 23
2.3.3. Versions of Internet Protocol 23
2.3.4. IP Version 4 23
2.3.5. The classes of IPv4 addresses 23
2.3.6. Private IP address 23
2.3.7. IP Version 6 24
2.4. Domain name System (DNS) Concepts: 24
2.4.1. Definitions 24
2.4.2. Domain Name Space 26
2.4.3. Before DNS 26
2.5. Web Hosting Concepts: 27
2.5.1. Website Hosting 27
2.5.2. Web Server 27
2.5.3. Web Host 27
2.5.4. Services are given by Web Hosting Companies 27
2.6. Domain Name Registration Process 27
2.6.1. Payment information 28
2.6.2. Registry 28
2.6.3. Registrar 28
2.6.4. Registrant 28
2.6.5. Difference between a Registry and a Registrar 29
2.7. Investigation procedure for Domain names 29
2.8. Email Concepts 31
2.9. Mail Server 32
2.10. How Does Email server work? 32

2.11. Email header 32
2.12. E-mail investigations 34
CHAPTER 3 35
Social Media Investigation 36
Why should you read this Chapter? 36
3. Introduction to Social Media 36
3.1. Different types of crimes reported on social media 37
3.1.1. Creating Impersonating/Fake accounts on Social Media 37
3.1.2. Cyber Stalking & Cyberbullying 37
3.1.3. Buying Illegal Things 37
3.2. Investigation procedures on Social media 37
3.3. Social Media monitoring and intelligence platforms 41
3.3.1. How does Social Media Monitoring work? 41
3.3.2. Social media monitoring tools: 41
CHA P TER 4 45
Communication device based Investigation 46
Why should you read this Chapter? 46
4. Introduction to communication devices 46
4.1. Understanding cellular networks 46
4.1.1. Information obtained from the network service provider 47
4.2. Laws related to Interception 48
4.2.1. Indian Telegraph (Amendment) Rules, ... 48
4.2.2. The laws and rules related to interception 51
4.2.3. Some important Definitions 52
4.2.4. Direction for interception or monitoring or decryption 52
4.2.5. Authorisation of agency of Government: 53
4.2.6. Issue of decryption direction by competent authority 53
4.2.7. Interception or monitoring or decryption of information 53
4.2.8. How to seek information from a mobile service provider? 53
4.3. Call Detail Record (CDR) 53
4.3.1. CDR formats 54
4.3.2. CDR Analysis 54
4.4. Other Mobile related investigations 58
4.4.1. Role of Tower dump analysis in investigations 58
4.4.2. Internet Protocol Detail Record (IPDR): 58
4.4.3. Voice over IP (VOIP) based investigations 59
4.4.4. Investigation of VOIP 59
4.5. Case study: Threating call over the internet 59

CHAPTER 5 60
Mobile Forensics 61
5. Introduction to mobile forensics 61
5.1. Major mobile phone related Cyber Crimes 61
5.2. Mobile Forensics definitions 62
5.2.1. Evidence in Mobile Devices 62
5.2.2. Evidence that can be extracted from a traditional mobile device 62
5.2.3. Evidence that can be extracted from a smartphone 62
5.2.4. Evidence related to the intermediaries 63
5.3. Types of memory on mobile phones 63
5.4. Techniques of Mobile Forensics 64
5.5. List of Mobile Forensics Tools 66
5.6. Challenges in extraction of Forensic evidence 66
5.7. Investigative Procedures 67
5.8. Steps involved in the analysis of mobile devices: 67
5.9. Precautions to be taken before an investigation 68
5.10. Scenario: If a mobile device is recovered from a bomb blast site 68
5.10.1. If Cell Phone is Switched On 68
5.10.2. If Cell Phone is OFF 68
CHAPTER 6 70
Investigation of Financial Frauds & cyber crimes 71
Why should you read this Chapter? 71
6. Introduction to investigation of cybercrimes & financial frauds 71
6.1. Steps to Follow in case of a fraudulent online transaction 71
6.2. Investigation of ATM withdrawal cases 71
6.3. Investigation of online transaction cases 71
6.4. Investigation of Bank to Bank transfer 71
6.5. Investigation transactions involving Cheques 72
6.6. Summary of common investigation steps 72
6.7. Indicative notice under 91 CrPC issued to the bank 72
6.8. Key Definitions 73
6.9. Key Abbreviations 73
6.10. Wallet transfers 73
6.11. Advance fee fraud 73
6.12. Lottery frauds 74
6.13. Job Frauds 74
6.14. Matrimonial Frauds 74
6.15. Loan Frauds 75

6.16. E-mail compromise frauds 75
CHAPTER 7 **..... 76**
Why should you read this Chapter? 77
7. Introduction to investigation abroad 77
Sec 187. Power to issue summons or warrant 77
Sec 166A – Letter of request to competent authority 78
105 B. Assistance in securing transfer of persons 78
Comprehensive Guidelines for Investigation Abroad 79
A. Investigation Abroad 79
B. Visit of Police Officers Abroad For Investigation 79
C. Investigation Abroad Under Section 166-A Crpc, 1973 80
D. Procedure To Be Followed After Issue Of LR By The Competent Court 83
E. Handling Of Incoming Letters Rogatory (LR) 83
F. Handling Of Extradition Requests 84
G. Contact By And With Foreign Police/ Legal Officers 84
CHAPTER 8 **..... 87**
Why should you read this Chapter? 88
8.1. Definitions Computer 88
8.2. The principles of digital evidence 89
8.3. Steps to follow in the scene of crime 89
8.4. Introduction to Hashing 92
8.4.1. Definition 92
8.4.2. Why Hashing? 92
8.4.3. Demonstration 92
8.4.4. Indicative Free tools 94
CHAPTER 9 **..... 95**
Why should you read this Chapter? 96
9.1. Introduction to Information Technology (IT) ACT: 96
9.2. Essence of information technology (IT) ACT 96
9.3. Important sections under IT Act for discussion: 97
Section 43: Penalty and Compensation for damage to computer, computer system, etc. 97
Section 66 Computer Related Offences 97
Section 66 B Punishment for dishonestly receiving stolen computer resource or communication device 97
Section 66C Punishment for identity theft 97
Section 66D Punishment for cheating by personation 98
Section 66E Punishment for violation of privacy 98
Section 66F Punishment for cyber terrorism 98

Section 67 Punishment for publishing or transmitting obscene material 99
Section 67 A Punishment for publishing or transmitting of material containing sexually explicit act, etc. 99
Section 67 B Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc. 99
Section 67 C Preservation and Retention of information by intermediaries..... 99
Section 69 Powers to issue directions for interception 100
Section 69 A Power to issue directions for blocking 100
Section 69B Power to authorize to monitor and collect traffic data..... 101
Section 72 Breach of confidentiality and privacy 101
Section 72A Punishment for Disclosure of information..... 101
Section 76 Confiscation 101
Section 77 B Offences with three years imprisonment to be cognizable 102
Section 78 Power to investigate offences 102
Section 80 Power of Police Officer and Other Officers to Enter, Search, etc. 102
Section 84 B Punishment for abetment of offences. 102
Section 84 C Punishment for attempt to commit offences 102
9.4. Other important provisions under Cr.P.C. 102
Section 165 Cr.P.C. Search by a police officer 102
Section 100 Persons in charge of closed place to allow search. 103
9.5. Admissibility of electronic records under Indian Evidence ACT 103
65A. Special provisions as to evidence relating to electronic record..... 104
65B. Admissibility of electronic records 104
9.6. Few illustrations were certificates u/s 65B IEA may be obtained 105
9.7. Mapping of the offences ITAA 2008 106
9.8. Cyber café guidelines 109
9.8.1. Short title and commencement. 109
9.8.2. Definitions 109
9.8.3. Agency for registration of cyber cafe. 110
9.8.4. Identification of User. 110
9.8.5. Log Register. 111
9.8.6. Management of Physical Layout and computer resource 112
***CHAPTER 10* 114**
***10. Case Study 1: Job Fraud* 115**
***10.1. Evidences provided by the complainant* 115**
10.1.1. More details on investigation..... 116
10.2. Case study 2: Sharing of morphed obscene contents..... 117
10.3. Case study 3: E-mail spoofing case 118
10.4. Case study 4: Matrimonial Fraud 119

10.5. Case study 5: Posting obscene content in yahoo group 120
10.6. Case study 6: Harassing a lady by posting obscene comments 121
Lab Exercises 123
Annexure 1 130
Annexure 2 131
Annexure 3 132
Annexure 4 133
(Lab Exercises) 133

Document Control

Document Information:

Owner	Ministry of Home Affairs
Document Status	Approved
Date Effective	12 November 2018

Document Revision History

Version No.	Status	Date	Author	Reviewed by	Approved by	Change Log
1.0	Final	12 November 2018	PMU	Advisor(ICT),MHA	JS,CIS,MHA	Version 1

Acknowledgement

The Ministry of Home Affairs (MHA) would like to thank the central training institutes, stakeholder Ministries, States, academia and professional bodies for recommending course structure for the program and state Law Enforcement Agencies for providing inputs and feedback for this book which is created, compiled and edited by CCPWC - PMU team MHA.

As per the Advisory released by MHA on 2/2/18 (F.No 22006/2/2017-CIS-II), a recommended training schedule is given under Annexure 4

CHAPTER 1:

Introduction to Cybercrimes

CHAPTER 1

Introduction to Cyber crimes

Why should you read this Chapter?

After reading this chapter, you would be able to:

- Understand about the various Cyber Crimes which could have potential impact on an individual or on an organisation.
- Identify ways through which Cybercrime could be carried out.
- Familiarize yourself on different Cyber security practices.

Introduction:

Internet connectivity is becoming ubiquitous and the technology integration is increasing into the lives of people and processes. Total number of internet users have increased from 1 billion in 2005 to more than 4 billion in December 2017[1]. As government goes digital with the digital India programme, the use of e-commerce, e-banking, e-Office, e-Health system, e-governance, e-KYC services etc., have encouraged citizens to go digital to perform day to day transactions.

Note: *US-CERT defines computer forensics as the discipline that combines elements of law and computer science to collect and analyse data from computer systems, networks, wireless communications, and storage devices in a way that is admissible as evidence in a court of law.*

The Government of India realized the need for introducing a law to facilitate e-commerce transactions and give legal recognition to electronic records and digital signatures.

The legal recognition to electronic records and digital signatures, in turn, will facilitate the conclusion of the contracts leading to creation of legal rights and obligations through the electronic communications.

As per reports from NCRB there has been a constant surge in cases of cybercrime reported in the last 4-5 years. The Government of India has led the fight against cybercrimes through the enactment of IT Act in the year 2000 and its amendment in the year 2008. Law enforcement agencies are facing challenges in fighting cybercrimes.

Training in cybercrime investigation techniques and cyber forensics to various stakeholders (involved in cybercrime investigation & prosecution) are very critical in combating cybercrimes.

In the current digital landscape, it would be practically impossible to retrieve the kind of evidence required to solve some of the cases reported to the law enforcement agencies. Cyber forensics is relatively new and constantly changing with the proliferation and introduction of new technologies.

A generalized definition of cybercrime may be “unlawful acts wherein the computer is either a tool or target or both[2].

[1] https://www.internetworldstats.com/stats.htm

[2] Cybercrime, Digital Forensics and Jurisdiction

Types of Cybercrimes

The methods and technologies cybercriminals use to commit their crimes are innumerable and continue to grow each year in both number and sophistication. Listed below are few common types of cybercrimes

1.1. Email related crime

The ease, speed and relative anonymity of email have made it a powerful tool for misuse by cyber criminals. Some of the major e-mail related crimes are given below:

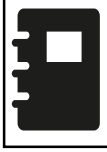
1.1.1. Email spoofing

Email spoofing is the forgery of an email header so that the message appears to have originated from someone or somewhere other than the actual source. Email spoofing is an approach used in phishing and spam campaigns because people are more likely to open an email when they think it has been sent by a legitimate source. There are different types of email spoofs, but they all have similarities. One main similarity is that you receive an email which claims to be from someone you know but in reality, it has been sent by another source.

1.1.2. Phishing/vishing

Phishing involves fraudulently acquiring (very often attacker try to disguise themselves and their communication as genuine) the sensitive information (e.g. online banking passwords, credit card details, debit card details etc.). The suspect's identity might be traced using the IP addresses of the suspected email sent.

If you click on a link in an email spoof, it might direct you to a fake webpage to collect your sensitive information.



Note: Always check the link before clicking. Hover over it to preview the URL, and look carefully in the email message for misspelling or other irregularities.

1.1.3. Email bombing

Email bombing is a form of an abuse consisting of sending huge volumes of email to a single address or recipient in an attempt to overflow the mailbox or overwhelm the server where the email address is hosted causing denial of service.

1.1.4. Spamming

Spamming is sending an unsolicited message, especially to promote a product or services, as well as sending messages repeatedly through a communication medium. Spammers not only use e-mail services but also use other channels such as SMS, TV advertising, social networking, Internet forums, Blogs etc.

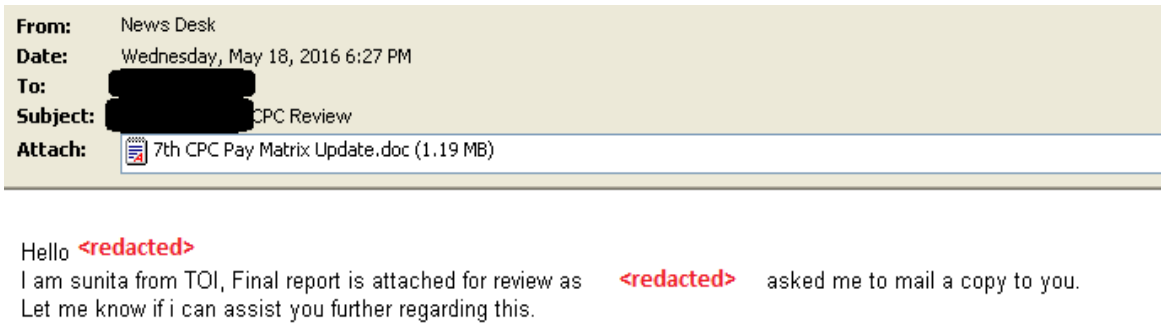
1.1.5. Spear phishing

It is a directed attack which is one of the very rampant email frauds till date. Spear phishing is a targeted phishing aimed at specific individuals or groups within an organization especially corporates. Spear phishing makes the use of information about a target to make attacks more

specific and personal to the target. Spear-phishing emails, for instance, may refer to their targets by their specific name, rank, designation or position instead of using generic titles as in normal phishing campaigns.

Spear-phishing emails can have malware attachments in the form of varying file types e.g. XLS, PDF, DOC, .DOCX etc. The malware then accesses a malicious command-and-control (C&C) server to take instructions from a remote user. At the same time, to hide malicious events malware usually drops a decoy document that will open when the malware or exploit runs.

For example, cyber criminals sent an MS word attachment titled '7th Central Pay Commission', knowing the high interest among government employees. These emails were generated over a fake domain timesofindiaa (note the extra letter 'a' in the end).



Source: Fire eye blog

1.2. Illegal Online transaction

Through illegal online transactions the perpetrator deprives the victim for funds, personal property, interest or sensitive information via the Internet. There are majorly three types of frauds:

- fraudulent or unauthorized transactions
- Lost or stolen merchandise
- False requests for a refund, return or bounced cheques

Fraudsters have become savvy at illegally obtaining information online. Cyber criminals often pose as a legitimate representative and contact credit/Debit card owners asking for sensitive information. They may use one or more of the following means of interaction to steal personal data:

- Email
- Texting malware on smartphones
- Instant messaging
- Rerouting traffic to fraudulent websites
- Phone calls

1.3. Job Frauds

It involves deceiving people seeking employment by giving them the false hope of earning high salaries or extra income. There are numerous methods where scammers come up with attractive offers such as easy hire, easy work, high wages, flexible working hours etc.,

1.4. Cyber defamation

As per Indian Penal Code (IPC) whoever, by words either spoken or intended to be read, or by signs or by visible representations, makes or publishes any imputation concerning any person intending to harm, or knowing or having reason to believe that such imputation will harm, the reputation of such person, is said to defame that person. Cyber defamation is the new form of committing traditional defamation where virtual communication like emails, Social Media, etc., is used to defame an individual or organization.

1.5. Ponzi scheme

A Ponzi scheme is a fraudulent investment scam where criminals lure the victims promising high rates of return with little risk.

e.g. Money Trade Coin (MTC) - A crypto currency scam estimated to be in the range of Rs 300 crore to Rs 500 crore.

1.6. Cyber stalking

Cyber stalking is a criminal practice in which attacker use internet and other electronic devices to persistently harass victims.

e.g. State of Maharashtra Vs Atul Ganesh Patil

A women had come for job interview to a company and wrote her mobile number in the entry register. The guard saved her contact details and started sending multiple obscene WhatsApp messages and even called her repeatedly to talk obscene things thereby committing crime of stalking her. In this case, victim blocked his number. However, the guard started sending her obscene messages from his friend's mobile phone. A case was registered under IPC 354D. The police acted swiftly completing the investigation and prepared a charge sheet within 24 hours.

1.7. Cyber bullying

It is a form of offense committed by using virtual communication medium like e-mail, social media, SMS, messengers, forums etc., to harass, threaten, embarrass, and humiliate victims. Cyber bullying can be anonymous or it can also have wider audience which can spread quickly. Cyber bullying commonly occurs among teenagers.

1.8. Cyber pornography

Cyber pornography is defined as the act of using cyberspace to create, view, distribute, import, or publish pornography or obscene materials.

1.9. Cybercrimes/Attacks of advanced types

Cybercriminals use various technologies to exploit security holes. These technologies are constantly growing in number and sophistication.

1.10. Hacking

It is an attempt to exploit weaknesses for gaining unauthorized access in a computer system or network. As per IT act, hacking is a term used to describe the act of destroying or deleting or altering any information residing in a computer resource or diminishing its value or utility, or affecting it injuriously in spite of knowing that such action is likely to cause wrongful loss or damage to the object, public or a person.

1.11. Virus

Computer Virus means any computer instruction, information, data or programme that destroys, damages degrades or adversely affects the performance of a computer resource. It generally attaches itself to another computer resource and operates when a programme, data or instruction is executed or some other event takes place in that computer resource.

1.12. Worm

It is a self-replicating malicious software that replicates itself to spread across other devices that are connected to a network.

1.13. Trojan

It is a malicious software that is camouflaged as a legitimate software e.g. Microsoft office, web browsers, media players, gaming applications etc. When this legitimate software installed the malicious code will also get installed at the background and start doing it's malicious activity.

1.14. Website defacement

It is an attack intended for a Website, which will change the visual appearance of a website and the attacker may post some other indecent, hostile and obscene images, messages, videos, etc., and sometimes make the Website dysfunctional.

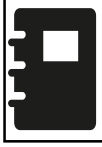
The most common cases of website defacement are, hackers of one country try to deface the websites of rival countries to display their technological superiority by infecting with malware.

1.15. Salami Attack

An attack is made on a system or network that involves making minor alteration so insignificant that in a single case it would go completely unnoticed. These attacks are generally used for the commission of financial crimes.

1.16. Cross-site scripting

Cross-Site Scripting (XSS) is a type of vulnerability in which malicious scripts are injected into content from otherwise trusted websites. The injection occurs when a user clicks on an unsuspected link that is specially designed for attacking a website they are visiting.



Note: Script is a sequence of commands or programs that are written in certain programming languages which may be used to automate certain process on the communication devices like smartphones, laptops, desktops etc.,

1.17. Web Jacking

The Web Jacking Attack is an advanced phishing technique where attackers make a clone of a website and send that malicious link to the victim. Once, the victims click the link that looks real he will be redirected to a fake page where attackers try to extract sensitive data such as card numbers, user names, passwords etc., from the victims.

1.18. DOS/DDOS attacks

In the Denial of service attack (DoS), an important service offered by a Web site or a server is denied or disrupted thereby causing loss to the intended users of the service. Typically, the loss of service is the inability of a particular network service, such as e-mail, to be available or the temporary loss of all network connectivity and services.

In some cases, DoS attacks have forced the Websites to temporarily cease operation. This often involves sending a large amount of traffic in the form e-mails and other requests to the targeted network or server so that it occupies the entire bandwidth of the system and ultimately results in a crash. The Distributed Denial of Service (DDoS) is a type of attack in which multiple systems are used by distributing the attaching BOTS to flood the bandwidth of the targeted system.

1.19. Ransomware

Ransom is defined as the practice of holding someone or something important to the victim with the intent to extort money or property to secure their release.

Ransomware is a type of computer malware that locks the files, storage media on communication devices like desktops, Laptops, Mobile phones etc., holding data/information as a hostage. There is no guarantee that the victim will get the data back after paying the ransom.

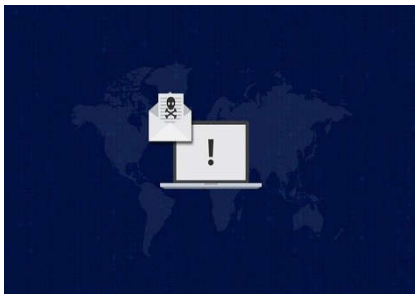


Fig: Ransomware

1.20. Data hiding technique

1.20.1. Steganography

Steganography is the practice of concealing a file, message, image, or video within another file, message, image, or video. The word steganography combines the Greek words steganos, meaning "covered, concealed, or protected," and meaning "writing".

Example of steganographed images

The below picture shows an image having hidden text inside a .png image.

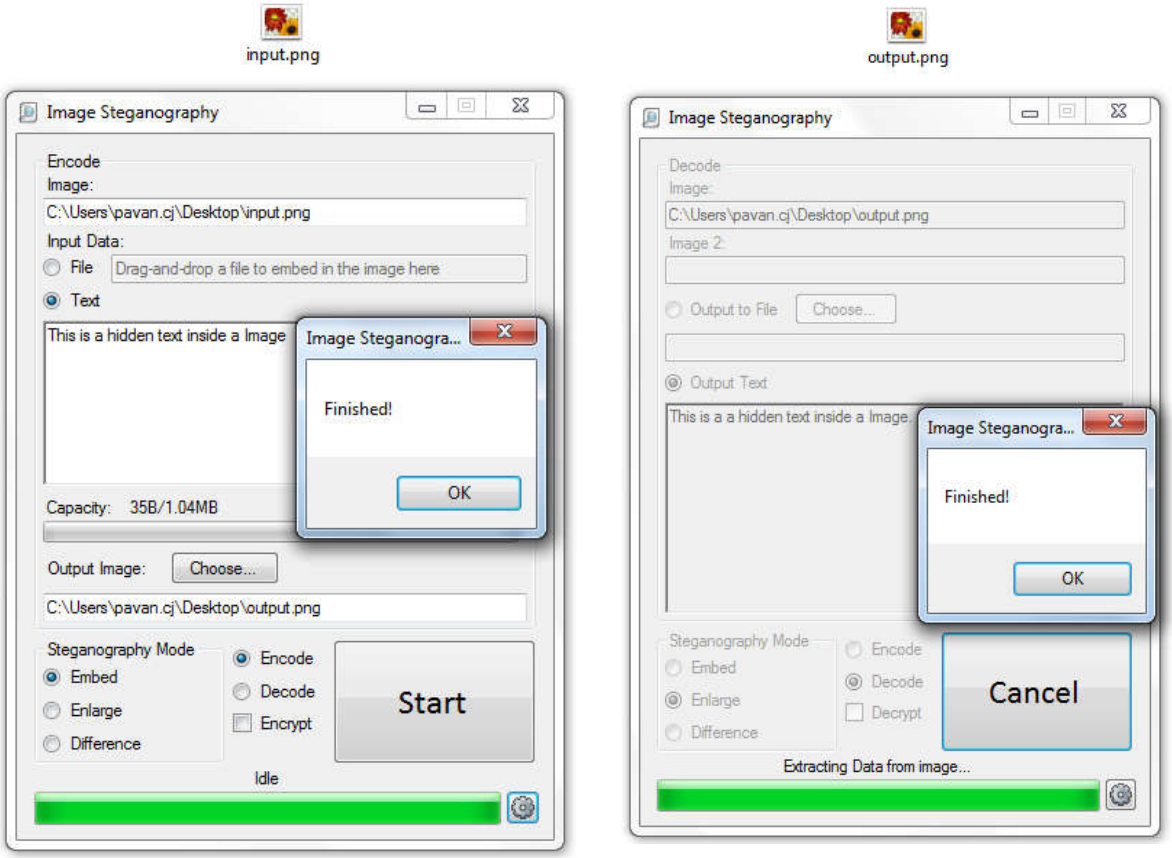


Fig: Data hiding using steganography

Note: Normally image, audio or video files are the standard cover files or the host files for embedding secret message such as text, image, audio or video. However, the size of the secret message must be very small in comparison to cover file. This method may be implemented in digital water marking in any legal documents, bank data transactions, etc.

1.21. Important concepts

1.21.1. Deep Web & Dark Web

The deep web is part of the internet where a typical search engine cannot index. The dark web/ darknets is a subset of deep web that is intentionally made hidden through overlay networks and require specific software, configurations or authorization to access.

Frauds are openly discussed on the underground forums of the Dark Web where illicit vendors offer fraudulent services. These services include but not limited to, launching a DoS attack on websites, the sale of malware, illegal drugs, weapons, cyber espionage on behalf of clients and the list goes on. Most of the vendors accept the payment through crypto-currencies and specially Bitcoins due to its popularity.

1.21.2. Cryptocurrency

Fig: Crypto Currency

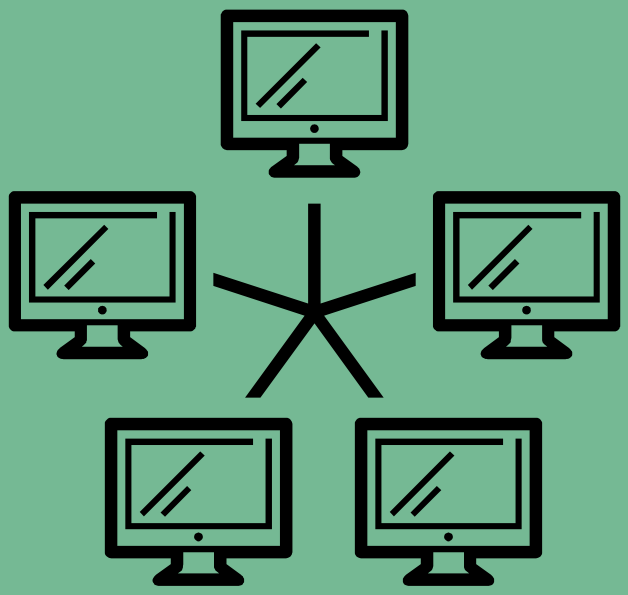
Cryptocurrency *Crypto* derives from Greek for *hidden* or *to hide.* A cryptocurrency is created by solving complex mathematical problem based on the cryptography to regulate the generation of units of currency and verify the transfer.

A cryptocurrency like Bitcoin consists of a network of peers. Every peer has a record of the complete history of all transactions and thus of the balance of every account. The validity of each cryptocurrency's coins is provided by a blockchain. A blockchain is a continuously growing list of records, called *blocks*, which are linked and secured using cryptography. Each block typically contains a hash pointer as a link to a previous block, a timestamp and transaction data. By design, block chains are inherently resistant to modification of the data. It is an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way.

User awareness – Safe practices to mitigate cybercrimes

The most effective mechanism to tackle cybercrime to be extra cautious in the cyberspace and promote the practices of netiquettes. Although these may sound very basic controls, it defends you on a larger scale. Few of them are listed as below:

- To avoid financial or banking related frauds never share OTP, PIN, password, card grid details, card expiry date, CVV number to anyone or entertain such calls impersonating as bank officials.
- Embed safe internet practices like avoid opening spam emails or attachments from an unknown source. Beware while opening external links or shortened URLs, as these might be phished or may infect your devices through malware.
- Apply a layer of personal protection on your devices by having up-to-date antivirus, licensed OS and software, secure your Wi-Fi and enable personal firewalls on laptops/computers
- Have strong passwords, enable privacy settings and cautiously post personal information and pictures.
- Never indulge in the distribution of obscene & illicit material.



CHAPTER 2

Computer Networks, E-mails & Web Hosting

CHAPTER 2

Computer Networks, E-mails & Web Hosting

Why should you read this Chapter?

After reading this Chapter, you would be able to

- Explore the communication mechanism used in various computer networks and the technologies related to it.
- Familiarize yourself with the key terms associated with the communication network and e-Mail
- Identify the communication networks and technologies from the cyber investigation perspective.

2. Introduction to computer networks

A computer network, often simply referred to as a network, is a collection of computers and devices interconnected by communications channels that facilitate communications among users and allows users to share resources. Networks may be classified according to a wide variety of characteristics.

2.1.1. Networking Requirements

Fig: switch

A network is a group of interconnected systems that share services and interact through a communications link. So, for a network to exist there must be two or more individual systems with something to share, like data. And, in order for these individual systems to share, they must be connected through some type of transmission medium. Now, if data is being sent over the transmission medium, all these individual systems must follow a set of common communication rules in order for the data to arrive at its intended destination or for the systems to properly understand each other. These rules that govern how the systems communicate are known as protocols.

Now, just having a transmission pathway should not suggest that communication is automatic because in order for two systems to communicate, they must be able to understand each other. The true goal of computer networking is not just to exchange data, but also to be able to understand and use the data that has been received.

So, below pointers taken together quickly summarize a network:

- Two or more individual systems
- Something to share
- A transmission medium
- Rules of communication or protocols

2.1.2. Connection method

Computer networks can be classified according to the hardware and software technology that is used to interconnect the individual devices in the network, such as optical fibre, Ethernet or wireless LAN.

Ethernet uses physical wiring to connect devices. Frequently deployed devices include hubs, switches, bridges, or routers. Wireless LAN technology is designed to connect devices without wiring. These devices use radio waves or infrared signals as a transmission medium. The technology uses existing home wiring (coaxial cable, phone lines, and power lines) to create a high-speed (up to 1 Gigabit/s) local area network.

2.1.3. Wired technologies (802.3)

Twisted pair wire is the most widely used medium for telecommunication. Twisted-pair wires are ordinary telephone wires which consist of two insulated copper wires twisted into pairs and are used for both voice and data transmission. The use of two wires twisted together helps to reduce crosstalk and electromagnetic induction. The transmission speed ranges from 2 million bits per second to 100 million bits per second.

Coaxial cable is widely used for cable television systems, office buildings, and other work sites for local area networks. The layers of insulation help minimize interference and distortion. Transmission speed range from 200 million to more than 500 million bits per second.

Optical fiber cable consists of one or more filaments of glass fiber wrapped in protective layers. It transmits light which can travel over extended distances. Fiber-optic cables are not affected by electromagnetic radiation. Transmission speed may reach trillions of bits per second

Wireless LANs (802.11) – Wireless local area network uses a high-frequency radio technology similar to digital cellular and a low-frequency radio technology. Wireless LANs use spread spectrum technology to enable communication between multiple devices in a limited area. Below table depicts the evolution of wireless standards

IEEE Standard	Frequency/Medium	Speed
802.11	2.4GHz RF	1 to 2Mbps
802.11a	5GHz	Up to 54Mbps
802.11b	2.4GHz	Up to 11Mbps
802.11g	2.4GHz	Up to 54Mbps
802.11n	2.4GHz/5GHz	Up to 600Mbps

Fig: Wireless standards

2.2. Types of networks based on the physical scope

Common types of computer networks may be identified by their scale.

2.2.1. Personal Area Network

A personal area network (PAN) is a computer network used for communication among computer and different information technological devices close to one person. Some examples of devices that are used in a PAN are personal computers, printers, fax machines, telephones, PDAs, scanners etc., A PAN may include wired and wireless devices. The reach of a PAN typically extends to 10 meters. A wired PAN is usually constructed with USB and Firewire connections while technologies such as Bluetooth and infrared communication typically form a wireless PAN.

2.2.2. Local Area Network

A local area network (LAN) is a network that connects computers and devices in a limited geographical area such as home, school, computer laboratory, office building, or closely positioned group of buildings. Each computer or device on the network is a node. Current wired LANs are most likely to be based on Ethernet technology, although new standards like ITU-T G.hn also provide a way to create a wired LAN using existing home wires (coaxial cables, phone lines and power lines).

2.2.3. Campus Network

A campus network is a computer network made up of an interconnection of local area networks (LAN's) within a limited geographical area. The networking equipment's (switches, routers) and transmission media (optical fiber, copper plant, Cat5 cabling etc.) are almost entirely owned (by the campus tenant/owner: an enterprise, university, government etc.).

In the case of a university campus-based campus network, the network is likely to link a variety of campus buildings including; academic departments, the university library, and student residence halls.

2.2.4. Metropolitan Area Network

A Metropolitan area network is a large computer network that usually spans a city or a large campus.

2.2.5. Wide Area Network

A wide area network (WAN) is a computer network that covers a large geographic area such as a city, country, or spans even intercontinental distances, using a communications channel that combines many types of media such as telephone lines, cables, and airwaves. A WAN often uses transmission facilities provided by common carriers, such as telephone companies. WAN technologies generally function at the lower three layers of the OSI reference model: the physical layer, the data link layer, and the network layer.

2.2.6. Virtual Private Network

A virtual private network (VPN) is a computer network in which some of the links between nodes are carried by open connections or virtual circuits in some larger network (e.g., the Internet) instead of by physical wires. The data link layer protocols of the virtual network are

said to be tunnelled through the larger network when this is the case. One common application is secure communications through the public Internet, but a VPN need not have explicit security features, such as authentication or content encryption. VPNs, for example, can be used to separate the traffic of different user communities over an underlying network with strong security features.

2.2.7. Peer-to-peer (P2P)

Computing or networking is a distributed application architecture that partitions tasks or workloads between peers. Peers are equally privileged, equipotent participants in the application. They are said to form a peer-to-peer network of nodes. Peers make a portion of their resources, such as processing power, disk storage or network bandwidth, directly available to other network participants, without the need for central coordination by servers or stable hosts. Peers are both suppliers and consumers of resources, in contrast to the traditional client-server model where only servers supply and clients consume.

Client-Server Architecture

The client-server model of computing is a distributed application structure that partitions tasks or workloads between the providers of a resource or service, called servers, and service requesters, called clients. Often clients and servers communicate over a computer network on separate hardware, but both client and server may reside in the same system. A server machine is a host that is running one or more server programs which share their resources with clients. A client does not share any of its resources, but requests a server's content or service function. Clients therefore initiate communication sessions with servers which await incoming requests.

Fig: Servers

2.3. The concept of IP address

The Internet Protocol Address (or ***IP Address***) is a unique address that computing devices such as personal computers, tablets, and smartphones use to communicate with other devices in the IP network. Any device connected to the IP network must have a unique ***IP address*** within the network.

The IP addresses can be classified into two. They are listed below.

1) Static IP addresses

2) Dynamic IP addresses

2.3.1. Static IP Addresses

As the name indicates, the static IP addresses are fixed IP addresses however, they can be changed as per the requirement or availability of IP address. They serve as a permanent Internet address and provide a simple yet reliable way of communication connected in a network

2.3.2. Dynamic IP Addresses

Dynamic IP address is a temporary IP addresses assigned to a computer, smartphones, tabs etc. when they get connected to the Internet each time. They are actually borrowed from a pool of IP addresses, shared over various computers. Since IPV4 is having a limited number of IP addresses, ISPs make a pool of IP addresses for sharing them among their subscribers.

2.3.3. Versions of Internet Protocol

The two versions of IP addresses currently running are IP versions 4 (IPv4) and IP versions 6 (IPv6).

2.3.4. IP Version 4

IP Version 4 (IPv4) was invented in 1970 and it was first introduced to the public on 1981. The IPv4 uses 32-bit IP address space capable of providing a maximum number of 2^{32} or 4,294,967,296 (~ 4 billion) IP addresses.

An IPv4 address is typically formatted as four 8-bit fields. Each 8-bit field is called an octet represents a byte (8 bits) of the IPv4 address.

E.g.: 182.151.36.24

2.3.5. The classes of IPv4 addresses

The different classes of the IPv4 address are the following:

Class	Range	Support
A	1.0.0.1 to 126.255.255.254	Large network
B	128.0.0.1 to 191.255.255.254	Medium Network
C	192.0.0.1 to 223.255.254.254	Small Network
D	224.0.0.1 to 239.255.255.255	Reserved for multicasting
E	240.0.0.1 to 254.255.255.254	Reserved for future & experimental use

2.3.6. Private IP address

According to standards set forth in Internet Engineering Task Force (IETF) document RFC-1918, the following IPv4 address ranges have been reserved by the Internet Assigned Numbers Authority (IANA) for private networks, and are *not* publicly routable on the global internet.

Host (Computers) that do not require access to hosts in other enterprises or the Internet at large; hosts within this category may use following IP addresses:

Class	**Start Range**	**End Range**
A	10.0.0.0	10.255.255.255
B	172.16.0.0	172.31.255.255
C	192.168.0.0	192.168.255.255

2.3.7. IP Version 6

The IPv6 is the most recent version of Internet Protocol. As the Internet is growing rapidly, there is a global shortage for IPv4. IPv6 uses a 128-bit address and it allows approximately 3.4×10^{38} addresses. The IPv6 addresses are represented by 8 groups of four hexadecimal digits with the groups being supported by colons. An example is given below:

E.g.: 2001:0db8:0000:0000:0000:ff00:0042:8329

DHCP: DHCP (Dynamic Host Configuration Protocol) is a network management protocol used to dynamically assign an Internet Protocol (IP) address to any device, or node, on a network so they can communicate using IP.

The DHCP server manages a pool of IP address and information about client configuration parameters such as default gateway, domain name, and the name servers. When a computer or other communication devices having networking capability connects to a network, the DHCP client software sends a broadcast query requesting necessary information. Any DHCP server on the network may service the request. On receiving a request, the server may respond with specific information for each client as configured by an administrator.

Note: Most of the internet service providers provide dynamic IP addresses to the end users. Investigators should take care of the date and time when they analyse any IP address during case investigation.

2.4. Domain name System (DNS) Concepts:

2.4.1. Definitions

Domain Name System (DNS) is a hierarchial distributed naming system for computers, services or any resource connected to a internet or a private network. It associates various informations with domain names assigned to each of the participating entities. Most prominently it translates domain names which can be easily memorized by humans to the numerical IP address needed for the purpose of computer services and devises world wide.

Note: Converts human readable names to machine readable IP address.
Or
A network service that translate “Names” to IP Address

Real world Scenario: DNS provides a name lookup facility that is similar to a standard telephone directory.

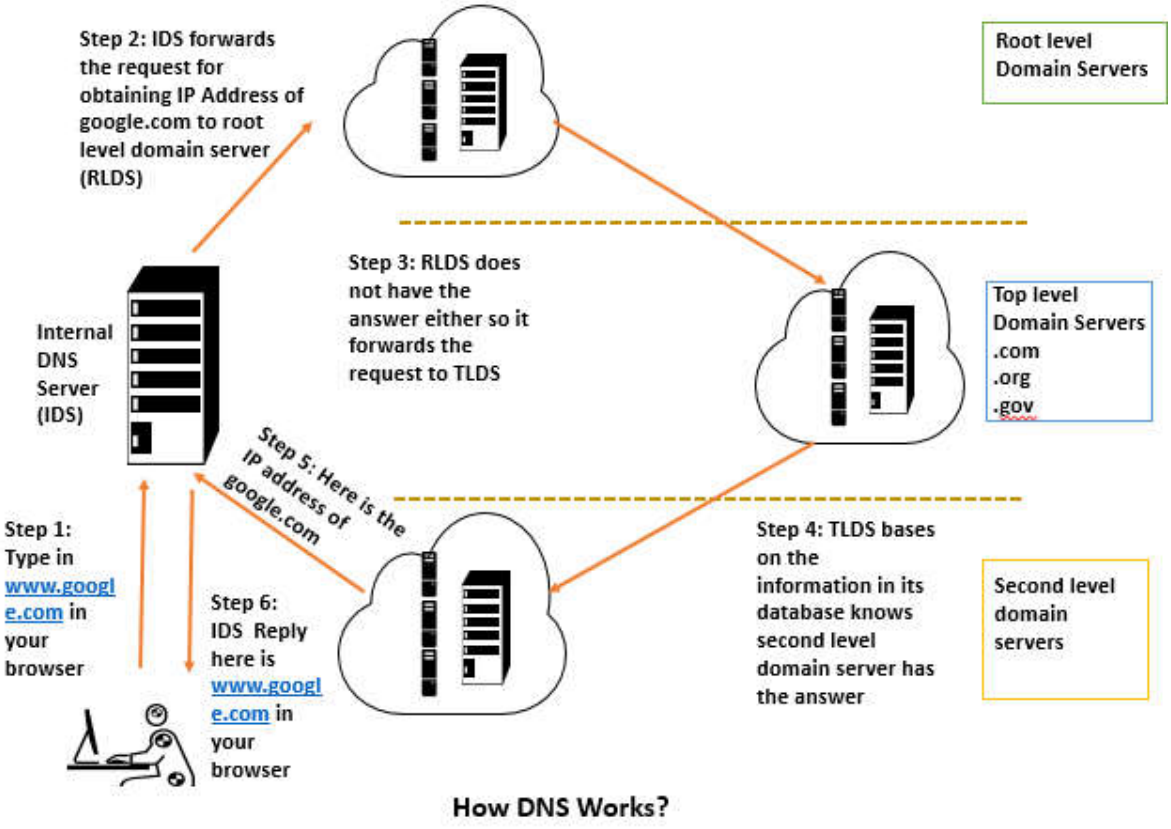


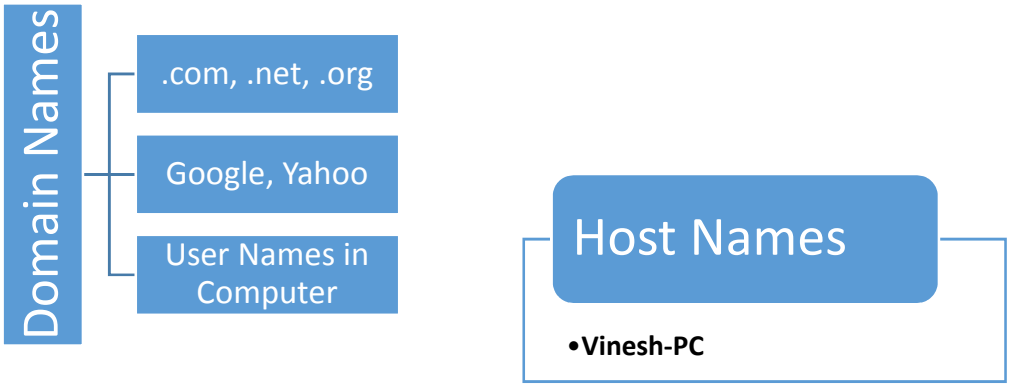
Fig: DNS Working

The three main components of a DNS system are:

Domain Name Space: defines the overall naming structure of the Internet

Name Server: maintains a portion of the domain name spaces, resolves lookups, and maintains a cache

Domain Name Resolution: maps a domain name to an IP address



Namespace:

Both the Hosts file and DNS use a namespace. A namespace is an environment created to hold group of related elements that each have a unique name or identifier. E.g. Domain names, File paths, XML document.

- ✓ Namespaces, such as DNS, are hierarchically structured and allows the namespace to be divided into subsets of names.
- ✓ Namespaces, such as the Hosts file, cannot be separated and the entire file should be distributed. This process posed a problem for network administrators.

As the number of computers and users on the Internet grew, it became difficult to manage with updating and distributing the hosts file in large networks.

DNS replaced traditional Hosts files with a distributed database that implements a hierarchical naming system. This naming system supported in the growth on the Internet by allowing to create unique names on the internet.

2.4.2. Domain Name Space

The domain name space defines the overall naming structure of the Internet. The name space comprises of a tree structure of domain names, with a root domain at the top. Immediately below the root domain are the major domains such as .com, .net, and .org. From these domains, the name space can branch into multiple paths, with each intersection point called a node and labelled with a simple name.

The structure of the DNS database, shown in Figure 1

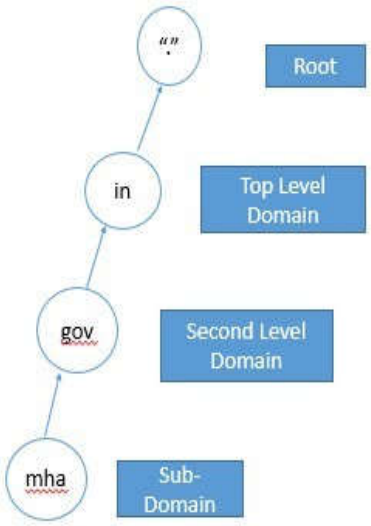


Fig: DNS hierarchy

Each domain can be further divided into additional partitions, called sub domains in DNS, like folders and sub folders in windows operating system. Subdomains, are like sub folders, are called as children of their parent domains.

In DNS, the domain name is the sequence of labels from root of the domain to the end of the whole tree, with dots (.) separating the labels.

2.4.3. Before DNS

A **host's file** is a list of computer names and their associated IP addresses. Hosts files are used by Microsoft Windows and other operating systems as a means to redirect internet traffic in network and applications.

Location of host file in windows: - C:\Windows\System32\drivers\etc

2.5. Web Hosting Concepts:

2.5.1. Website Hosting

Hosting a website means making a website available to public worldwide. When a website is created, it is composed of multimedia contents (text, images, videos and other content for people to see them. However, people can see your website only when it is available on the Internet. To make your website available on the Internet, you have to store it on a computer called web server. When you buy some space on a web server and store your web pages there, your website becomes hosted and can be seen by anyone.

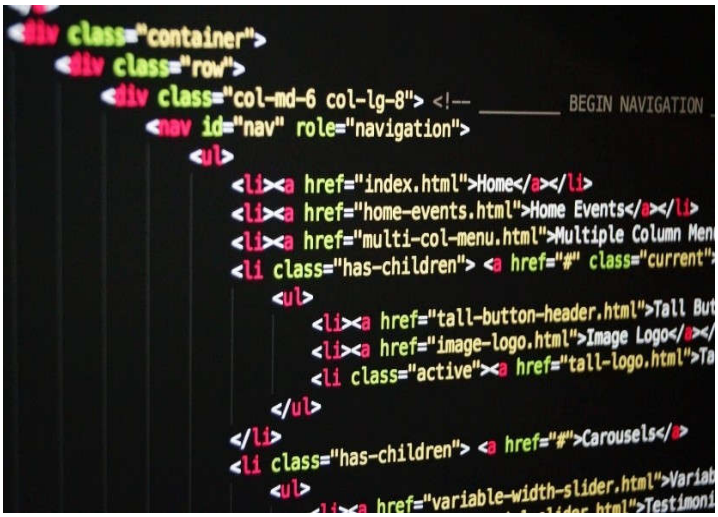


Fig: Sample source code

2.5.2. Web Server

A web server is a computer on which the web pages of your website are stored. It delivers or 'serves' the content of your website to the users through the Internet. The web hosting companies will be owning an array of servers on which they offer renting out space for their clients. After purchasing of space, the users can now host their website and make it accessible to the public.

2.5.3. Web Host

Any person or company who owns a server and rents out web space for website hosting can be called the web host. Some companies will not be having the required servers and infrastructure, however, rent a server/space from a large web hosting company and then resell the space under their own brand. This is called *reseller hosting service* and such web hosts are called web resellers. Many of the web hosting companies not only provide web space but offer many other services related to website hosting and are thus also called web service providers.

2.5.4. Services are given by Web Hosting Companies

Space on their servers is the most important service offered by a web hosting companies. There exist many other products and services offered by web hosting companies that are essential for website hosting such as domain name registration, e-mail services, and SSL certificates etc. Some of the service providers also offer web designing tools having some templates where the user can choose them to create a website.

2.6. Domain Name Registration Process

A user can choose a domain name. The chosen name should be submitted to a registrar as a domain name registration request.

The following information is required for creating a website:

- The desired domain name e.g. mytravel.com, vinesh.in, agrosolution.org
- The name and contact information (including email address, physical address and contact phone number) for the domain's registrant, administrative and billing contacts.
- The desired domain registration term e.g. duration, additional services etc.

2.6.1. Payment information

After receiving the above information registrar will initiate the domain name registration process. The registrar will send the domain name request, contact and technical information of the domain name to the registry.

The registry file will be having the contact information for the WHOIS. The registry also adds the requested domain to the zone files to the master servers. The master servers communicate with other servers on the Internet where the website is stored.

2.6.2. Registry

A registry is a company or organization that maintains a centralized registry database for the Top-Level Domains. Currently, there is only one Registry for every Top-Level domain, .com, .net and .org. NSI Registry maintains this Registry.

2.6.3. Registrar

A registrar is an ICANN accredited company or organization that is authorized to provide registration services for the top-level domains such as .com, .org, .net etc. Registrars have contractual agreements with their customers.

A Registrar submits all newly registered domains into the Registry.

2.6.4. Registrant

The Registrant is the owner of a Domain Name. The owner may be an individual or an organization to which a specific Domain Name is registered.

When a Registrant registers a Domain Name and enters a contractual agreement with the Registrar, they are the legal owner of a domain name for a specific period of time. For example, Vinesh (Registrant) registers the name 'vinesh.com' through the Registrar who in turn writes the name to the central database (NSI Registry).

ICAAN

The Internet Corporation for Assigned Names and Numbers formed in October 1998, is a non-profit, private sector corporation with a volunteer board of directors. ICANN was formed with the chief responsibility for coordinating four key functions for the Internet:

- The management of the Domain Name System
- Allocation of IP address space
- Assignment of protocol parameters
- Management of the root server operators.
- For a company or organization to operate as a Registrar, they must first sign a Registrar Accreditation Agreement (RAA) with ICANN for accreditation.

2.6.5. Difference between a Registry and a Registrar

A registry provides direct services to registrars only, not Internet end-users. The Registry database contains only Domain Name service (DNS) information (Domain Name, name server names and name server Internet Protocol IP address) along with the name of the Registrar It does not contain contact information of a Registered Name Holder (Registrant).

A Registrar provides direct services to Domain Name registrants. The Registrar database contains customer information in addition to the DNS information contained in the registry a database. Registrars process the domain names requested by the users for registration and then send the necessary DNS information to Registry thus, by making the website available to the general public.

2.7. Investigation procedure for Domain names

1. Identify the website name (full URL) in question
2. Search for the registrar information using a WHOIS lookup
3. Identify the hosting company location and details
4. Serve notice requesting registrant (Registered name holder) of the website.
5. Serve notice for web hosting companies requesting registration details of registrant (IP address, Payment information, Mailbox contents if available, contact information)
6. Identify IP address form the logs obtained from the service providers
7. Search for the IP address in question using a WHOIS lookup
8. Identify the service provider
9. Serve notice for requesting physical address.

Serve notice under 79(3) (b) since, web hosting providers are defined as intermediaries under section 2 (w) of IT act.

- To get the physical address of the IP logs shared by the service provider
- To get the CAF & CDR of the registrant (If available)
  E.g. cases where child pornography (CP)/ Rape & Gang Rape Videos (RGR) hosted on a website

Tip: The following sites can be used for domain & IP address searching

- https://www.whois.com/whois
- www.whois.net
- http://whois.domaintools.com/domaintools.com

Note: If the websites are hosted outside India, MLAT process needs to be followed to get the details of the registrant. The MLAT procedures are discussed in detail later in the book

General Data Protection Regulation (GDPR) is introduced to standardize data protection laws applicable to EU data subjects. It is aimed to enhance privacy protection and was enforced from 25 may 2018. A data processor processes personal data only on behalf of a data controller, meaning personal information cannot be shared or published without the owner's permission impacting the information available on the WHOIS database.

Sample 79 (3) (b) notice is given below for your reference.

Office of Nodal Officer, , (State name) Police, Government of ……..
<Address…….>

To

<.Details of Intermediary
……..>

Subject: Notice/direction in terms of provision of Section 79 of the Information Technology Act, 2000 read with The Information Technology(Intermediaries Guidelines) Rules, 2011 for Removal of unlawful content & providing the relevant evidence for the investigation/prosecution of the Case FIR no.-----

It is hereby brought to your notice that contents hosted on <URL/user ID> are unlawful content as per section/s <67A/67B….or any other applicable section> of IT Act 2000/any other Act for which FIR ---- has been registered and under investigation, the sections are reproduced below for ready reference:

< Text of applicable sections of law >

1. The said illegal content has been caused to be published by your website on the internet for which you are liable to be prosecuted subject to your compliance to the provision of section 79(2)(c) & (3)(b) of the Information Technology Act, 2000 read with The Information Technology(Intermediaries Guidelines) Rules, 2011

2. In terms of the above provisions, , you are hereby directed to expeditiously remove access to the aforesaid illegal material/content mentioned above within a period of 36 hours without vitiating the evidence in any manner:

3. Further in terms of the rule 7 of The Information Technology(Intermediaries Guidelines) Rules, 2011 and the Section 91 of the Code of Criminal Procedure, 1973, you are requested to provide the following information which is required for the purpose of investigation & prosecution in the aforementioned case:-

   < Details of information sought>

4. Failure to comply with the aforesaid directed issued in terms of the provision of section 79 IT Act, 2000 will make you liable to be prosecuted for the abetment(Sec 84) or conspiracy or committing the offence mentioned in the aforesaid FIR subject to the outcome of the investigation.

Further failure to comply with the direction under section 91 of Cr.P.C is a punishable offence under section 174 of Indian Penal Code.

5. Compliance within stipulated period may please be ensured and compliance reported to this office.

Nodal Cyber Cell, Government of ……..
<Address…….>

Search result of:
www.svpnpa.gov.in

```
Domain ID:D12051-AFIN
Domain Name:SVPNPA.GOV.IN
Created On:28-Feb-2004 05:00:00 UTC
Last Updated On:28-Feb-2018 22:33:02 UTC
Expiration Date:28-Feb-2020 05:00:00 UTC
Sponsoring Registrar:National Informatics Centre (R12-AFIN)
Status:OK
Reason:
Status:RENEWPERIOD
Status:AUTORENEWPERIOD
Registrant ID:R-R04021716337
Registrant Name:Sardar Vallabhbhai Patel National Police Academy
Registrant Organization:
Registrant Street1:Shivram Palli
Registrant Street2:
Registrant Street3:
Registrant City:Hyderabad
Registrant State/Province:Andhra Pradesh
Registrant Postal Code:500052
Registrant Country:IN
Registrant Phone:+91.0424015151
Registrant Phone Ext.:
Registrant FAX:+240.15179
Registrant FAX Ext.:
Registrant Email:administrator@svpnpa.gov.in
Admin ID:A-R04021716337
Admin Name:M Gnana Seelan System Admin
Admin Organization:SVPNPA
Admin Street1:Shivarampally
Admin Street2:
Admin Street3:
Admin City:Hyderabad
Admin State/Province:Andhra Pradesh
Admin Postal Code:500052
Admin Country:IN
Admin Phone:+91.4024015151
Admin Phone Ext.:
Admin FAX:+91.4024015179
Admin FAX Ext.:
Admin Email:administrator@svpnpa.gov.in
Tech ID:T-R04021716337
Tech Name:Same As Above
Tech Organization:SVPNPA
Tech Street1:Shivaram Palli
Tech Street2:
Tech Street3:
Tech City:Hyderabad
```

Search result of IP
address 47.31.160.63

```
% [whois.apnic.net]
% Whois data copyright terms    http://www.apnic.net/db/dbcopyright.html

% Information related to '47.31.0.0 - 47.31.255.255'

% Abuse contact for '47.31.0.0 - 47.31.255.255' is 'ip.abuse@ril.com'

inetnum:        47.31.0.0 - 47.31.255.255
netname:        RELIANCEJIO-IN
descr:          Reliance Jio infocomm ltd
country:        IN
admin-c:        RJIL1-AP
tech-c:         RJIL1-AP
status:         ALLOCATED NON-PORTABLE
mnt-by:         MAINT-IN-RELIANCEJIO
mnt-irt:        IRT-INFOTELR4G-IN
last-modified:  2016-06-28T02:22:58Z
source:         APNIC

irt:            IRT-INFOTELR4G-IN
address:        Reliance Jio Infocomm Ltd RCP Ghansoli
e-mail:         ip.management@ril.com
abuse-mailbox:  ip.abuse@ril.com
admin-c:        IBSP1-AP
tech-c:         IBSP1-AP
auth:           # Filtered
mnt-by:         MAINT-RELIANCE-INFOTEL-IN
last-modified:  2013-07-29T09:16:31Z
source:         APNIC

role:           Reliance Jio Infocomm Limited
address:        Reliance JIO INFOCOMM LTD GHANSOLI INDIA
country:        IN
phone:          +91-44770000
e-mail:         ip.management@ril.com
admin-c:        RJIL1-AP
tech-c:         RJIL1-AP
nic-hdl:        RJIL1-AP
mnt-by:         MAINT-IN-RELIANCEJIO
last-modified:  2016-03-09T23:55:07Z
source:         APNIC

% Information related to '47.31.0.0/16A555836'

route:          47.31.0.0/16
descr:          Route Set JIO Delhi-2 LTE USER Pool
origin:         AS55836
mnt-by:         MAINT-IN-RELIANCEJIO
notify:         ip.abuse@ril.com
last-modified:  2016-06-28T03:11:07Z
source:         APNIC

% This query was served by the APNIC Whois Service version 1.88.15-43 (WH
```

2.8. Email Concepts

Email is also called as electronic mail. It is similar to postal service mail, but much quicker to use. For instance, with postal service mail, you write out a letter and put it inside an envelope, put a stamp on the envelope, take the envelope to a mailbox and wait several days for the envelope to be delivered and read. Email is quicker. Open your email program on a computer with a couple of mouse clicks. Compose a letter in the text message box. Type in the email address of your receiver. Click on Send. The person receives the email almost instantly.

Today's email systems are based on a store-and-forward model. Email servers accept, forward, deliver, and store messages. Neither the users nor their computers are required to be online simultaneously; they need to connect only briefly, typically to a mail server or webmail interface, for as long as it takes to send or receive messages. Functions such as email exchange are built on the client-server model.

2.9. Mail Server

A mail server is an application that receives an incoming e-mail from local users and remote senders and forwards outgoing e-mail for delivery. A computer dedicated to running such applications is also called a mail server. Microsoft Exchange, Gmail, Exim and send mail are among the more common mail server programs. The mail server works in conjunction with other programs to make up what is sometimes referred to as a messaging system. A messaging system includes all the applications necessary to keep e-mail moving as it should. When you send an e-mail message, your e-mail program, such as Outlook or webmail, forwards the message to your mail server, which in turn forwards it either to another mail server or to a holding area on the same server called a message store to be forwarded later. As a rule, the system uses SMTP (Simple Mail Transfer Protocol) or ESMTP (extended SMTP) for sending e-mail, and either POP3 (Post Office Protocol 3) or IMAP (Internet Message Access Protocol) for receiving e-mail.

2.10. How Does Email server work?

E-mails are communicated between two or more users. An e-mail can be composed by a sender using outlook, webmail or Application using computers, smartphones, tablets etc., Once the sender clicks the send button e-mail will be sent to the mail server. Every e-mail service providers (ESP) have their own dedicated e-mail servers which transfer e-mail from one part of the world to another.

When the mail server receives the e-mail message from the sender the destination address is verified, if the ESP is of the same company then the mail server can directly send it to the recipient's mailbox. If the recipients ESP is different, the sender's e-mail server will look for the recipient's e-mail server and send to that e-mail server. The receivers e-mail server then pushes the e-mail to the recipient. As the message travels through the network, an abbreviated record of the e-mail journey is recorded in an area of message called the header.

2.11. Email header

In most of the cybercrime where e-mails are involved, analysis of e-mail headers plays a very important role. Each e-mail whether it is a company e-mail or Web-based e-mail like Hotmail, yahoo, etc., carries lot of information about that e-mail. Information like sender IP address, e-mail address, time and date when the e-mail sent, through which server it passed, etc.

E-mail header analysis may help an investigator to find out the IP address of the e-mail sender (Source IP). Headers record important information, including servers that the e-mail has travelled through, and the date and time that the message was received or forwarded.

Every email service provider is having the option to view senders e-mail headers. The headers can be easily analysed. The following procedure can be followed for header analysis:

1. Select the sender e-mails ID where the header is required for the investigation and extract the full header information. Copy the header information on a notepad, WordPad, MS-Word or any other word processing program. Below steps demonstrates how to view full headers on Yahoo mail.

Select a recipient whose e-mail you want to analyse and open that mail and select more option.

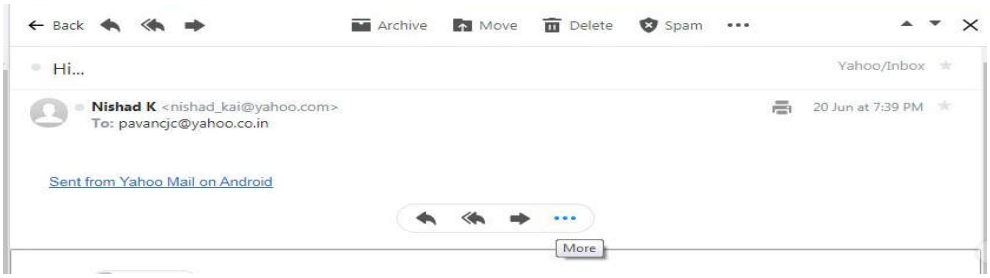


Fig 1 selecting more option by clicking on "…" symbol

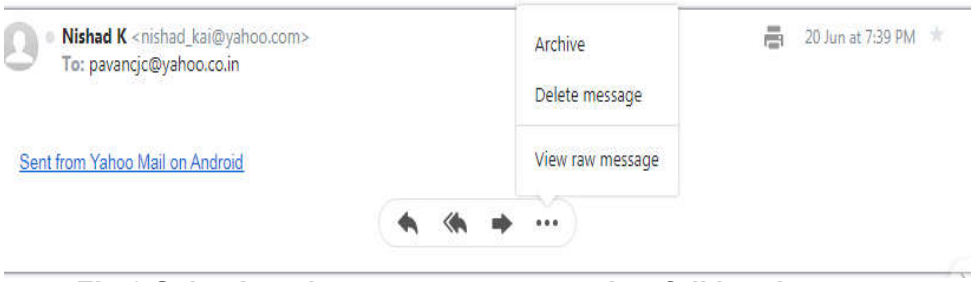


Fig 2 Selecting view raw message to view full header

2. Search for online header analyser on Google, Bing or any other search engine of your choice. Some examples are
    a. https://www.whatismyip.com/email-header-analyzer/
    b. https://mxtoolbox.com/EmailHeaders.aspx

The below figures shows the copied email header pasted by selecting option a mentioned in the example for analysis.

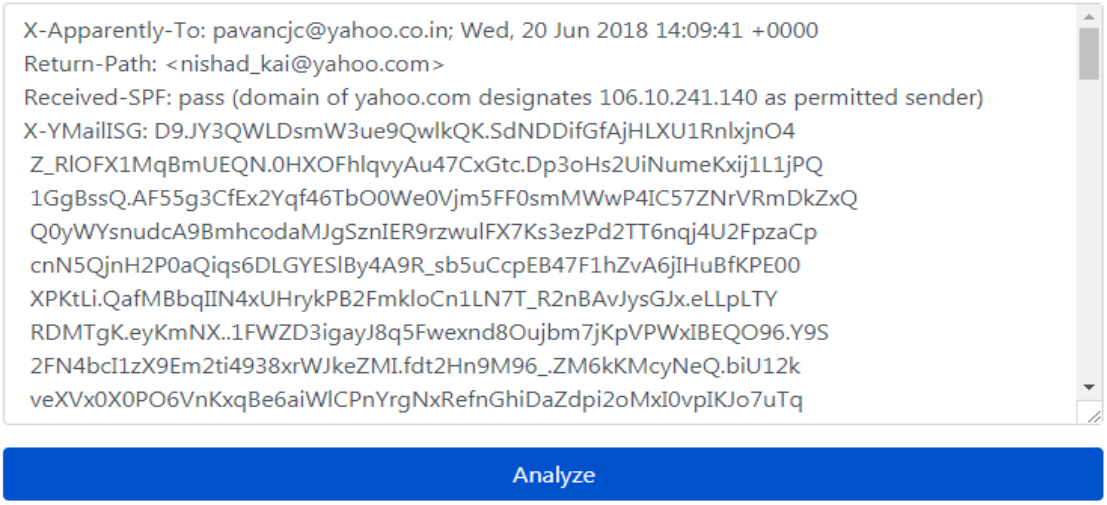


Fig 3: Paste the header in the box and click on analyse

3. Paste the header in the box and press analyse the header

Fig 4: e-mail source IP

2.12. E-mail investigations

- Identify senders e-mail ID
- Extract the header information from the complainant and identify the source IP address
- Request for registration and access details
- Request for mailbox contents
- Do a WHOIS search of IP address and identify service providers
- Send notices under Cr.P.C. 91 requesting physical address of the user

Tip: Most of the e-mail service provider started replacing the senders IP with their own servers IP or Private IP address. To get the sender IP from the ESP, request them for Registration and access details of an e-mail ID under 91 CrPC

CHAPTER 3

Social Media Investigation

CHAPTER 3

Social Media Investigation

Why should you read this Chapter?

After reading this Chapter, you would be able to understand

- The major types of crime reported on social media
- Investigation procedures on social media
- Introduction to social media analysis & tools of the trade
- Reporting a fake Facebook profile

3. Introduction to Social Media

Social networking is one of the leading online activities worldwide. There are more than 2.46 billion social network users worldwide in 2017 with more than 64 percent of internet users accessing social media services online. In 2020, experts estimate 2.95 billion people to access social networks regularly. The majority of this growth is projected to come from mobile devices, as emerging markets catch up on online connectivity.

Social networking is one of the most popular ways for online users to spend their time, enabling them to stay in contact with friends and families as well as catching up with news and other content.

Popular social media sites

Sl. No	Social Media	Statistics
1	 [3]	**As per the Facebook report[4]** **Daily active users (DAUs)** – DAUs were 1.40 billion on average for December 2017, an increase of 14% year-over-year. **Monthly active users (MAU)** – MAUs were 2.13 billion as of December 31, 2017, an increase of 14% year-over-year.
2	 [5]	Every second, on average, around 6,000 tweets are tweeted on Twitter which corresponds to over 350,000 tweets sent per minute, **500 million tweets per day** and around 200 billion tweets per year.
3	 [6]	YouTube has revealed that a billion hours are spent on the video streaming site each day[7].
4		Instagram has 1 billion Monthly Active Users. [8] 855 Instagram photos uploaded in 1 second.

[3] https://www.flaticon.com/free-icon/facebook_174848#term=facebook&page=1&position=2
[4] https://investor.fb.com/investor-news/press-release-details/2018/Facebook-Reports-Fourth-Quarter-and-Full-Year-2017-Results/default.aspx
[5] https://www.flaticon.com/free-icon/twitter_174876
[6] https://www.flaticon.com/free-icon/youtube_174883#term=youtube&page=1&position=2
[7] https://www.indiatoday.in/technology/news/story/youtube-videos-are-watched-for-one-billion-hours-every-day-963089-2017-02-28
[8] https://techcrunch.com/2018/06/20/instagram-1-billion-users/

Social networking allows users to create an online profile through which they will share or post personal and professional information about them. This includes pictures, videos, and other personally identifiable information. Undoubtedly, social media is becoming the scene of the crime in many types of emerging crimes.

3.1. Different types of crimes reported on social media

Below you'll find four common crimes being committed on, or as a result of, social media.

1. **Creating Impersonating/Fake accounts on Social Media**
2. **Online Threats, Stalking, Cyberbullying**
3. **Buying Illegal Things**

3.1.1. Creating Impersonating/Fake accounts on Social Media

Impersonating/Fake profiles on social media like Facebook, google plus, twitter etc. is a problem that most of the users face in their daily life. Creating fake accounts or impersonating accounts is a punishable offense. In most of the cases, the purpose of making an impersonated social media profile is to harass and defame the victim. Fake accounts are created to commit the crimes such as cyberstalking, cheating, post defamatory images, post defamatory articles against an individual, organization or government, create communal hatred contents, create hoax information etc.,

E.g. Thousands of panic-stricken people of the northeast living in Bengaluru boarded trains, headed to Guwahati, in the year 2012, following rumors of violence targeting them. Hoaxes and fake videos like this travel so fast that they need to be controlled and regulated immediately when they are happening to be out and trending.

3.1.2. Cyber Stalking & Cyberbullying

Cyberstalking and bullying which are two very real dangers that can haunt victims in both virtual and physical environment. Cyberstalking refers to foster personal interaction repeatedly targeting a person despite the clear indication of disinterest by such person. In many cases, men/women's social media accounts are stalked by their ex-partners. Cyberbullying is the use of technology to harass, threaten, embarrass or target another person. Cyberbullying is a serious problem among teenagers.

3.1.3. Buying Illegal Things

Social media allows creating closed groups, communities of like-minded people on many social media networks to discuss events, the topic of interest (such as movies, technology, TV series etc.). This is also an opportunity for many sellers to come online and sell contraband items, alcohol, arms, fake goods such as sports shoes, watches, sunglasses, designer wear, gadgets bags of famous brands etc.,

3.2. Investigation procedures on Social media

While registering FIR for any cybercrime, (whether it is social media or job fraud or email threatening or any other digital crime), precautions should be taken for collection of information from complainant and service provider. Let's take a typical example of the fake profile created in the name of the complainant and understand the investigation procedure.

1. Any case investigation will be started with information gathering from the complainant. For cases like fake profiles, self-attested printout copies of the fake profile need to be printed (where profile ID needs to be clearly mentioned). Soft copies of offensive chat or messages along with the date and time stamps need to be collected.

2. Investigation officer (IO) can request for registration details of the fake profile created by the accused. Details may include:
    a. Name
    b. Date of Birth
    c. IP Address
    d. Date and time the profile was created
    e. Email ID if any when the profile was created
3. The above details can be requested using one of the following methods:
    - Issue a code of criminal procedure (CrPC.) notice under section 91 to the service provider with the above details
    - Some service providers offer portals to request for details specific to law enforcement. An IO can directly go to the respective portal and upload the notice.

A sample copy of the CrPC 91 notice is given below for your reference.

CYBER CRIME POLICE STATION,
[redacted]

Cr.No.202[redacted] /2016, Date:

Notice U/Sec. 91 Cr.P.C.

I am the Superintendent of Police working at Cyber Crime Police Station, CID, [redacted] India. I am investigating a case wherein a complainant named [redacted] who is working for reputed company, has found her personal photos posted with 2 profiles. The postings contains her personal photos and contains vulgar title [redacted]. Hence the details are very much essential for the purpose of investigation. The URL of the Facebook profiles is appended below for your reference.

https://www.facebook.com/profile.php?id=[redacted]

https://www.facebook.com/profile.php?id=1[redacted]

In this connection it is requested to furnish the **Registration & accessing IP Log details** of the above said profile including dates & timings for the purpose of investigation. You are further requested to remove the said profile soon after furnishing of information.

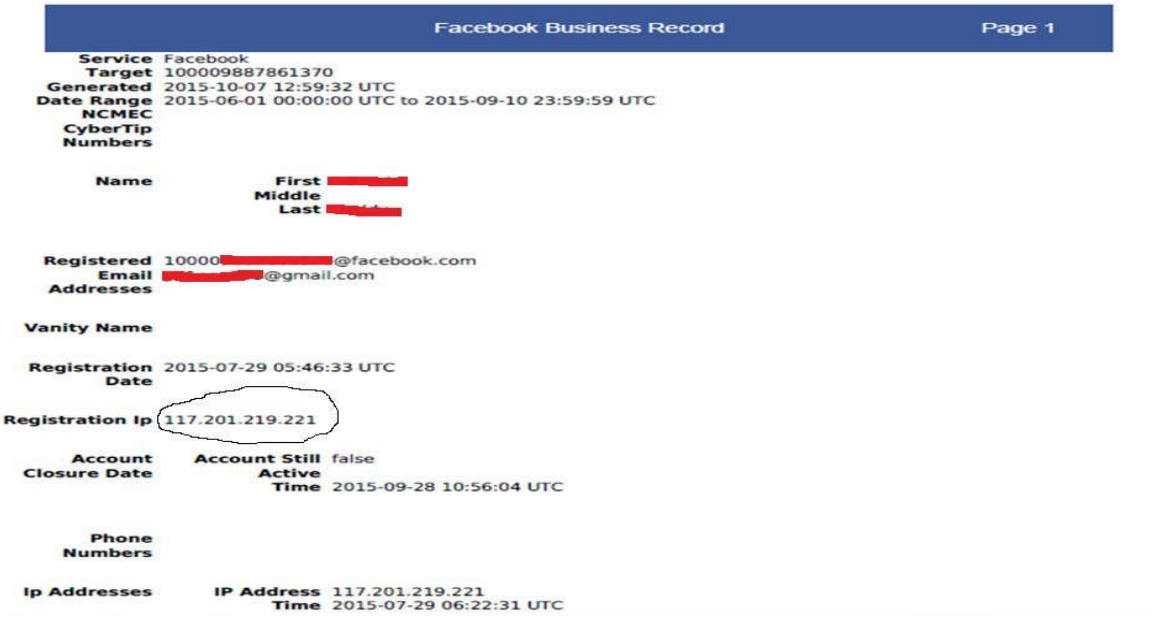
[redacted]

SUPERINTENDENT OF POLICE,
[redacted]

To
Facebook Ireland Ltd
4 Grand Canal Square
Dublin 2

Below is the reference of the law enforcement portal created by the Facebook for requesting the suspected user details:

- The response from the service provider can be downloaded from the portal. Below is the reference screenshot with corresponding details.



4. Upon collecting the information about the related details like name, IP address, date of creation etc. from the service provider, IO should plan for requesting physical location details of the IP address obtained from the above report as per the legal provisions under Cr P.C.
5. Email service provider can also be approached to obtain information of the user which was found in the above report. Similar kind of CrPC. 91 notice is sent to the email service provider to obtain the IP address of the accused behind the crime. This will be helpful to make the case stronger with enough evidence and collate the data for the trial.
6. IP addresses obtained from the service providers are verified for WHOIS information from any WHOIS website. This gives the internet service provider details of that particular IP.
7. Upon collecting the information about the IP address from the internet service provider or based on local investigations about the relevant scene of offense, the IO has to plan his actions for search/ seizure as per the legal provisions under Cr PC.
8. Once at the suspected place of offense, the IO should identify the computer or mobile or any digital device used by the accused. The digital evidence needs to be seized by following the best practices of search and seizure.
9. To determine whether seized digital evidence from accused contained evidence regarding usage of the system for creating the fake profile and uploading the offensive photographs of the complainant using any tools or morphing software. Ensure that all the details relevant are furnished along with the expert opinion request.
10. The I.O has to brief the jurisdictional court and obtain a search warrant to perform search & seizure of the premises where IP address is traced.
11. The accused must be arrested and remanded to the court, based on the investigations and evidence collected. The IO has diligently worked along with technical experts to map the information from the social networking site company, ISP, and other service providers.
12. It is very important that all the evidence are collected with timestamps and converted into Indian Standard Time (IST). A majority of the service providers are international companies and record the time in their own time standards (UTC/GMT, PST etc.)
13. The IO will send the seized articles for forensic examination by preparing a questionnaire related to the case.
14. The investigator was given a report describing the findings of the examination. The forensic examination will confirm the role of accused and also reveal the usage of any other software used by the accused.

3.3. Social Media monitoring and intelligence platforms

It is very vital to understand how social media is changing and so the cybercrimes committed through social media and their impact on one's life. Perpetrators being young or old commit crimes without hesitation, whereas outside the internet, in real life, they have to assume the power of consequences bears a heavier weight.

3.3.1. How does Social Media Monitoring work?

Methodologically, social media monitoring can be performed in the following two ways.

- The first involves feeding the algorithm with a string of keywords, which leads to "producing an overview of the instances of online communication and their locations (forums, Facebook pages, Twitter accounts, etc.) in which these keywords are used".
- The second way entails directing the algorithm towards a specific set of discussion forums and social networking sites, and to search them for a number of keywords. As opposed to traditional forms of monitoring, social media monitoring is real-time and continuous.

Social media monitoring techniques have their origins in the private sector. These practices were, aimed at market research and customer profiling. But with time, law enforcement agencies have recognized their utility.

3.3.2. Social media monitoring tools:

There are two types of tools available to monitor social media:

1. **Sentiment analysis:**

   Sentiment analysis refers to the class of computational and natural language processing study of people's opinions, appraisals, and emotions toward events, institutions or other subject matter in order to extract subjective information, such as opinions expressed in a given piece of text.

2. **Social network analysis:**

   Social network analysis is a technique used to map and measure social relations. They are used as investigative tools to discover, analyze, and visualize the social networks of criminal suspects.

   However, it is important to consider how the scope of surveillance discretion changes with the use of new technologies such as predictive policing and social media monitoring tools.

Social Media Tools

Name	Type	Description
Advanced Application for Social Media Analytics	Free*	Advanced Application for Social Media Analytics (AASMA) is the tool for social media monitoring and analysis. It is developed at IIIT Delhi and funded/supported by Ministry of Electronics and Information Technology (MeitY)
X1 Social discovery	Commercial	Ability to collect and search data from social networks and the Internet.
Maltego	Commercial/ Freeware available with limited caps	It is an open source intelligence gathering tool capable of a significant amount of information gathering about a prospective target
Amped Authenticate	Commercial	Amped Authenticate is a software package for forensic image authentication and tamper detection on digital photos. Authenticate provides a suite of different tools to determine whether an image is an unaltered original, an original generated by a specific device, or the result of a manipulation with a photo editing software.
Hootsuite	Commercial	Social media management platform. The system's user interface takes the form of a dashboard, and supports social network integrations for Twitter, Facebook, Instagram, LinkedIn, Google+, YouTube etc.,
SocialPilot	Commercial	Measure your social media page's performance by understanding the growth of your fans/audience. Also, understand what content works the most with users from social networking audience. It provides insights for Twitter, Facebook, Instagram, LinkedIn, Google+, YouTube etc.,
Netglub	Open source	Open source tools for information gathering. It collects open data like DNS name, Domain name, IP address, IP Sub network, Message Exchanger record, Nameserver Record, Url, Website
Poortego	Open source	Open source tools for visualizing and linking the information available online.

Scenario: Reporting fake profile on Facebook

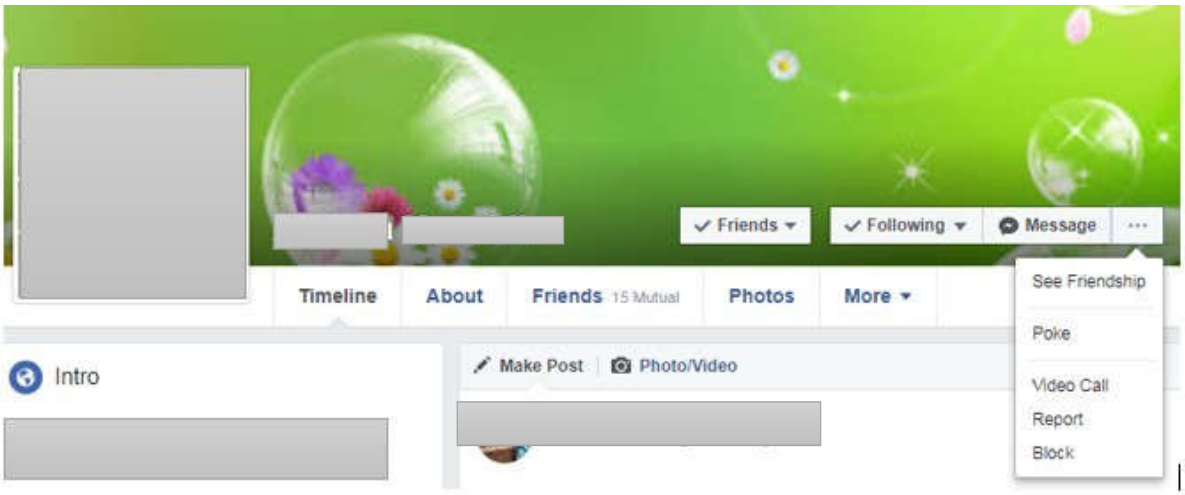
The IO can educate the victims to utilize block and report option on Facebook to stop further victimization.

For example, in the case of Facebook the following procedure has to be followed to report an abusive page:

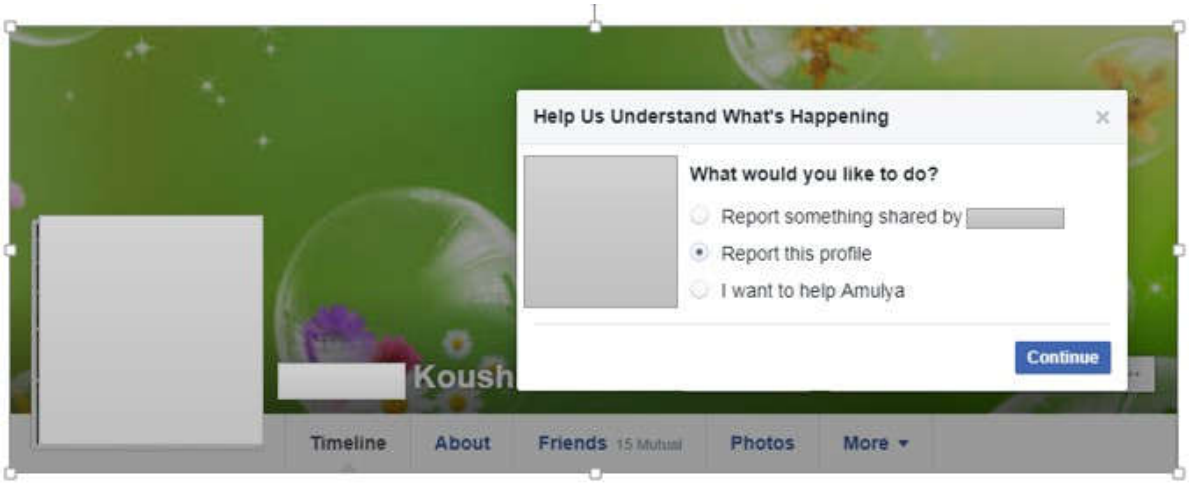
- Go to the Page you want to report
- Click the gear icon below the Page's cover photo
- Select Report Page
- Choose the reason you're reporting the Page and click Continue.

Step 1: Identify the profile you want to report

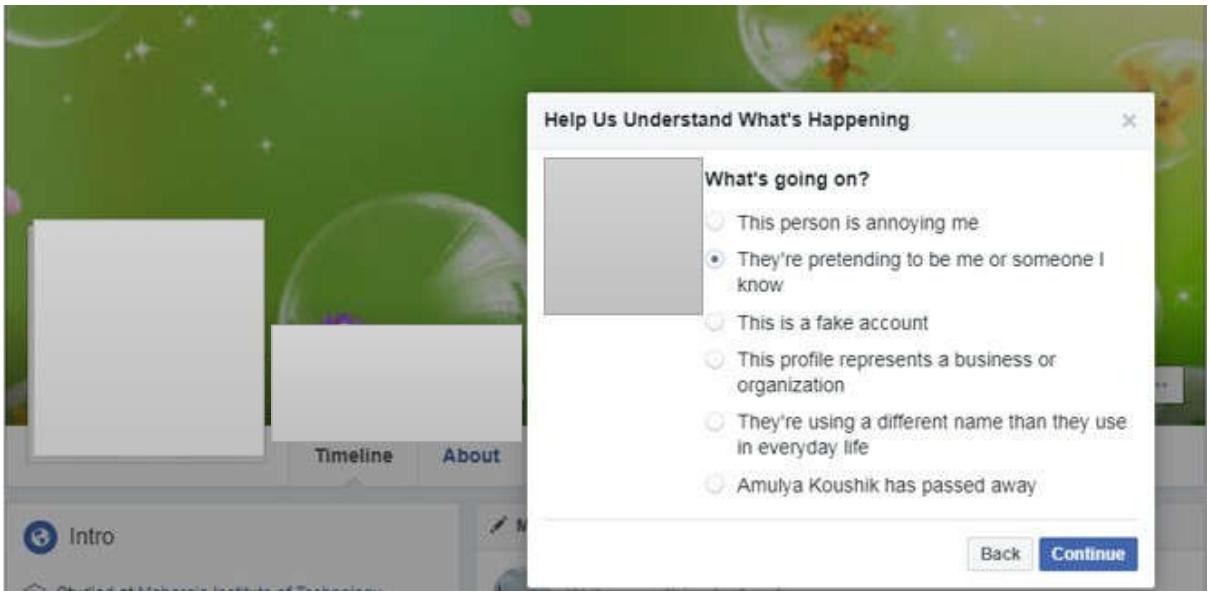
Step 2: Select **Block** if you want to Block the person. In this scenario, we are reporting the person



Step 3: Click on the report this profile

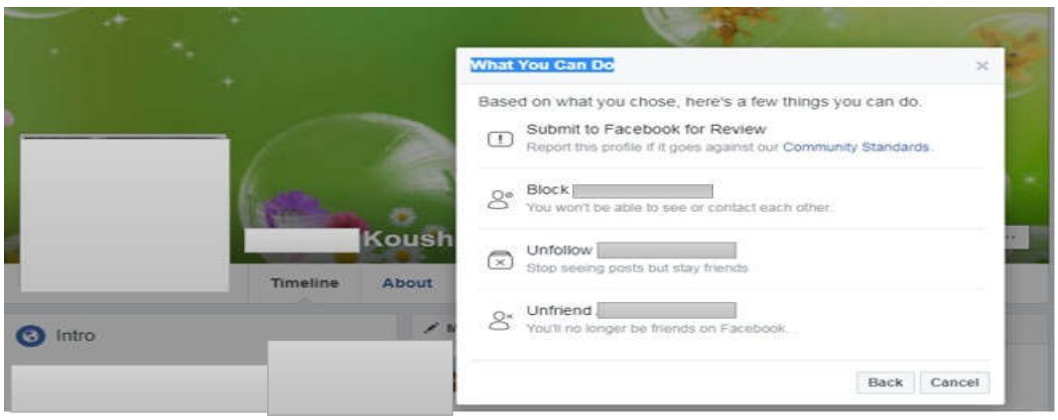


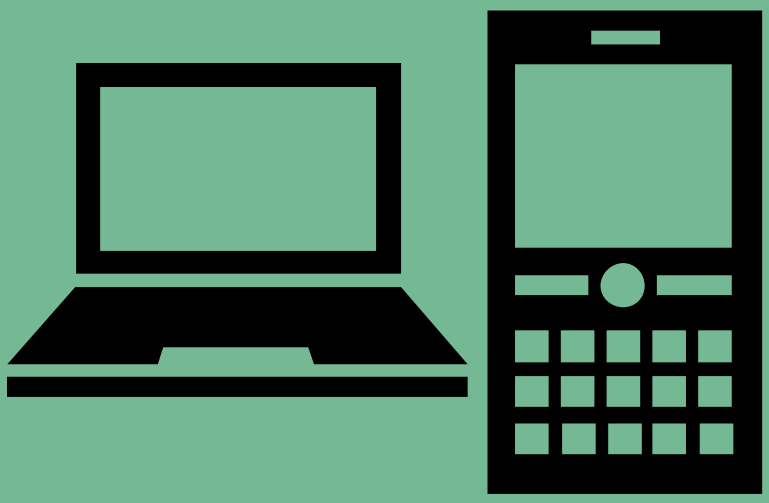
Step 4: You will get the following options. Here impersonation is being reported



Step 5: Select the appropriate option based on the case.

Step 6: Select submit to Facebook for review





CHAPTER 4

Communication device based Investigation

CHAPTER 4

Communication device based Investigation

Why should you read this Chapter?
The goal of this chapter is to introduce you to how communication happens between various devices especially Mobile phones and Investigation techniques associated with it.

After reading this chapter, you would be:

- Familiarized with mobile forensic and challenges associated with it.
- Familiarized with the technical know-how of a mobile phone and different types of data generated during the investigation.
- Familiarized with CDR, IPDR, VOIP concepts.
- Able to perform basic analysis using MS-excel

4. Introduction to communication devices

As per IT Act, “communication device" means cell phones, personal digital assistants or combination of both or any other device used to communicate, send or transmit any text, video, audio or image.

Primarily cell phones/mobile phones are considered as communication devices in our daily life. A mobile/cell phone is an electronic device. It works on radio signals & used for personal communication over remote distances. For easy understanding of investigation, we are discussing mobile phones as the communication device further in this document. Mobile phones can provide several different kinds of forensic evidence which may be electronic or physical. Mobile Forensics is discussed in detail later in this book.

4.1. Understanding cellular networks

As the name implies, cellular networks provide coverage based on dividing up a large geographical service area into smaller areas of coverage called cells. Cells play an important role in the reuse of radio frequencies in the limited radio spectrum available to allow more calls to occur than otherwise would be possible.

As a mobile device moves from one cell to another, a cellular arrangement requires active connections to be monitored and effectively passed along between cells to maintain the connection. To administer the cellular network system, provide subscribed services, and accurately bill or debit subscriber accounts, data about the service contract and associated service activities is captured and maintained by the network system.

The main components are the radio transceiver equipment that communicates with mobile devices, the controller that manages the transceiver equipment and performs channel assignment, and the switching system for the cellular network. Each Mobile Switching Center (MSC) controls a set of Radio Network Controller (RNC) and manages overall communications throughout the cellular network, including registration, authentication, location updating, handovers, and call routing.

A key database is the central repository system for subscriber data and service information, called the *Home Location Register (HLR)*. Another database used in conjunction with the HLR is the *Visitor Location Register (VLR),* which is used for mobile devices roaming outside of their service area. Account information, such as data about the subscriber (e.g., a billing address), the subscribed services, and the location update last registered with the network are maintained at the HLR and used by the MSC to route calls and messages and to generate usage records called Call Detail Records (CDR). The subscriber account data, CDRs, and related technical information obtained from the network carrier are often a valuable source of evidence in an investigation.

4.1.1. Information obtained from the network service provider

- Subscriber name and address
- The phone number associated with SIM
- Billing account details
- Call Data Record
- IMSI – International Mobile Subscriber Identity
- ICCID – Integrated Circuit Card ID
- PUK (Personal Unlocking Key) for the SIM.
- Tower Location (BTS Address)
- Subscribed Services (Voice Mails, Caller-tunes, Classifieds, etc.)

The picture given below is the telephone architecture of how a public switching telephone network works:

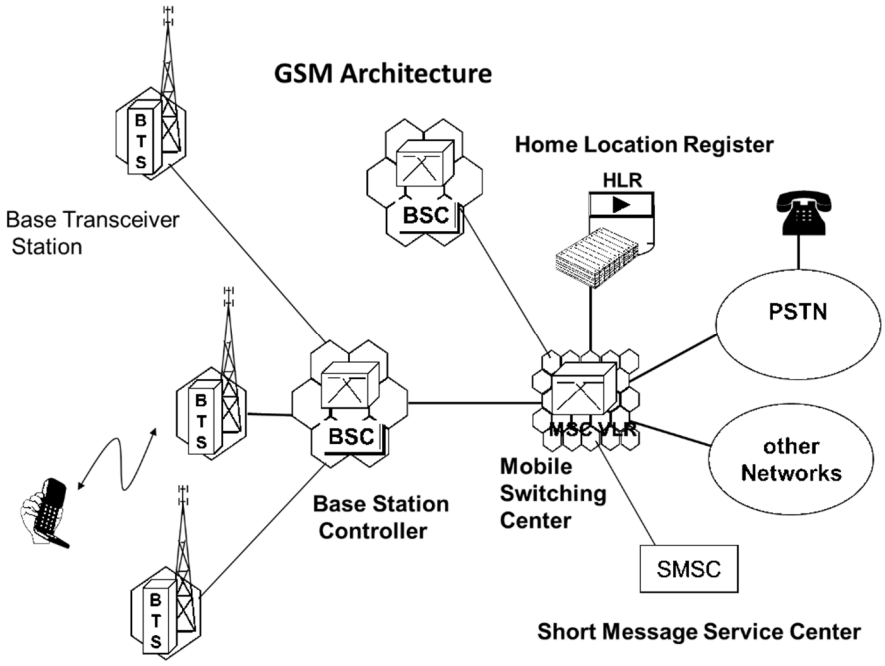


Fig: GSM Architecture

The below table will explain you the frequency of the GSM and CDMA technologies:

	GSM	CDMA
	Global System for Mobile Communication	Code Division Multiple Access
Handset Identity / Serial Number	International Mobile Equipment Identity (IMEI)	Electronic Serial Number (ESN)
Subscriber Identity	International Mobile subscriber Identity (IMSI)	Mobile Identification Number (MIN)
Frequency	**900 Band** 890-915 MHz (Uplink) 935-960 MHz (Downlink) **1800 Band** 1710-1785MHz(Uplink) 1805-1880MHz(Downlink)	824-849 MHz (Uplink) 869 -894 MHz(Downlink)

Tip: You can always refer to the back panel of the phone or wireless hotspot for the IMEI number. You can also type *#06# to get the IMEI information. Alternatively, you can visit websites like http://www.imei.info/ to get more information on certain mobile phones.

4.2. Laws related to Interception

Lawful interception of telephonic communication is governed by the provisions of Section 5(2) of the Indian Telegraph Act, 1885, which empowers the Central and State Governments to carry out interception of communication messages under the stipulated conditions. The detailed procedure for handling the lawful interception cases is provided in Rule 419A of Indian Telegraph (Amendment) Rules, 2007.

4.2.1. Indian Telegraph (Amendment) Rules, 2007. 419-A.

(1) Directions for interception of any message or class of messages under sub-section (2) of Section 5 of the Indian Telegraph Act, 1885 (hereinafter referred to as the said Act) shall not be issued except by an order made by the Secretary to the Government of India in the Ministry of Home Affairs in the case of Government of India and by the Secretary to the State Government in-charge of the Home Department in the case of a State Government. In unavoidable circumstances, such order may be made by an officer, not below the rank of a

Joint Secretary to the Government of India, who has been duly authorized by the Union Home Secretary or the State Home Secretary, as the case may be:

Provided that in emergent cases:
(i) In remote areas, where obtaining of prior directions for interception of messages or class of messages is not feasible; or
(ii) For operational reasons, where obtaining of prior directions for interception of message or class of messages is not feasible;
the required interception of any message or class of messages shall be carried out with the prior approval of the Head or the second senior most officer of the authorized security i.e. Law Enforcement Agency at the Central Level and the officers authorized in this behalf, not below the rank of Inspector General of Police at the state level but the concerned competent authority shall be informed of such interceptions by the approving authority within three working days and that such interceptions shall be got confirmed by the concerned competent authority within a period of seven working days. If the confirmation from the competent authority is not received within the stipulated seven days, such interception shall cease and the same message or class of messages shall not be intercepted thereafter without the prior approval of the Union Home Secretary or the State Home Secretary, as the case may be.
(2) Any order issued by the competent authority under sub-rule (1) shall contain reasons for such direction and a copy of such order shall be forwarded to the concerned Review Committee within a period of seven working days.
(3) While issuing directions under sub-rule (1) the officer shall consider the possibility of acquiring the necessary information by other means and the directions under sub-rule (1) shall be issued only when it is not possible to acquire the information by any other reasonable means.
(4) The interception directed shall be the interception of any message or class of messages as are sent to or from any person or class of persons or relating to any particular subject whether such message or class of messages are received with one or more addresses, specified in the order, being an address or addresses likely to be used for the transmission of communications from or to one particular person specified or described in the order or one particular set of premises specified or described in the order.
(5) The directions shall specify the name and designation of the officer or the authority to whom the intercepted message or class of messages is to be disclosed and also specify that the use of intercepted message or class or messages shall be subject to the provisions of sub-section (2) of Section 5 of the said Act.
(6) The directions for interception shall remain in force unless revoked earlier, for a period not exceeding sixty days from the date of issue and may be renewed but the same shall not remain in force beyond a total period of one hundred and eighty days.
(7) The directions for interception issued under sub-rule (1) shall be conveyed to the designated officers of the licensee(s) who have been granted licenses under Section 4 of said Act, in writing by an officer not below the rank of Superintendent of Police or Additional Superintendent of Police or the officer of the equivalent rank.
(8) The officer authorized to intercept any message or class of message shall maintain proper records mentioning therein, the intercepted message or class of messages, the particulars of persons whose message has been intercepted, the name and other particulars of the officer or the authority to whom the intercepted message or class of messages has been disclosed, the number of copies of the intercepted message or class of messages made and the mode or the method by which such copies are made, the date of destruction of the copies and the duration within which the directions remain in force.

(9) All the requisitioning security agencies shall designate one or more nodal officers not below the rank of Superintendent of Police or Additional Superintendent of Police or the officer of the equivalent rank to authenticate and send the requisitions for interception to the designated officers of the concerned service providers to be delivered by an officer not below the rank of Sub-inspector of Police.
(10) The service providers shall designate two senior executives of the company in every licensed service area/State/Union Territory as the nodal officers to receive and handle such requisitions for an interception.
(11) The designated nodal officers of the service providers shall issue acknowledgment letters to the concerned security and Law Enforcement Agency within two hours on receipt of intimations for an interception.
(12) The system of designated nodal officers for communicating and receiving the requisitions for interceptions shall also be followed in emergent cases/unavoidable cases where prior approval of the competent authority has not been obtained.
(13) The designated nodal officers of the service providers shall forward every fifteen days a list of interception authorizations received by them during the preceding fortnight to the nodal officers of the security and Law Enforcement Agencies for confirmation of the authenticity of such authorizations. The list should include details such as the reference and date of orders of the Union Home Secretary or State Home Secretary, date and time of receipt of such orders and the date and time of Implementation of such orders.
(14) The service providers shall put in place adequate and effective internal checks to ensure that unauthorized interception of messages does not take place and extreme secrecy is maintained and utmost care and precaution is taken in the matter of interception of messages as it affects privacy of citizens and also that this matter is handled only by the designated nodal officers of the company.
(15) The service providers are responsible for actions for their employees also. In case of established violation of license conditions pertaining to maintenance of secrecy and confidentiality of information and unauthorized interception of communication, action shall be taken against the service providers as per Sections 20, 20-A, 23 & 24 of the said Act, and this shall include not only fine but also suspension or revocation of their licenses.
(16) The Central Government and the State Government, as the case may be, shall constitute a Review Committee. The Review Committee to be constituted by the Central Government shall consist of the following, namely:

Central Government	
Cabinet Secretary	Chairman
Secretary to the Government of India In charge, Legal Affairs	Member
Secretary to the Government of India, Department of Telecommunications	Member
State Government	
Chief Secretary	Chairman
Secretary Law/Legal Remembrancer In charge, Legal Affairs	Member
Secretary to the State Government (other than the Home Secretary)	Member

(17) The Review Committee shall meet at least once in two months and record its findings whether the directions issued under sub-rule (1) are in accordance with the provisions of sub-

section (2) of Section 5 of the said Act. When the Review Committee is of the opinion that the directions are not in accordance with the provisions referred to above it may set aside the directions and orders for destruction of the copies of the intercepted message or class of messages.
(18) Records pertaining to such directions for interception and of intercepted messages shall be destroyed by the relevant competent authority and the authorized security and Law Enforcement Agencies every six months unless these are, or likely to be, required for functional requirements.
(19) The service providers shall destroy records pertaining to directions for interception of message within two months of discontinuance of the interception of such messages and in doing so they shall maintain extreme secrecy.

4.2.2. The laws and rules related to interception and monitoring under IT (Amendment) act, 2008 are given below

Section 69 Powers to issue directions for interception or monitoring or decryption of any information through any computer resource

(1) Where the Central Government or a State Government or any of its officer specially authorized by the Central Government or the State Government, as the case may be, in this behalf may, if is satisfied that it is necessary or expedient to do in the interest of the sovereignty or integrity of India, defense of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence relating to above or for investigation of any offence, it may, subject to the provisions of sub-section (2), for reasons to be recorded in writing, by order, direct any agency of the appropriate Government to intercept, monitor or decrypt or cause to be intercepted or monitored or decrypted any information transmitted received or stored through any computer resource.

Section 69B: Power to authorize to monitor and collect traffic data or information through any computer resource for Cyber Security

(1) The Central Government may, to enhance Cyber Security and for identification, analysis and prevention of any intrusion or spread of computer contaminant in the country, by notification in the official Gazette, authorize any agency of the Government to monitor and collect traffic data or information generated, transmitted, received or stored in any computer resource.
(2) The Intermediary or any person in-charge of the Computer resource shall when called upon by the agency which has been authorized under sub-section (1), provide technical assistance and extend all facilities to such agency to enable online access or to secure and provide online access to the computer resource generating, transmitting, receiving or storing such traffic data or information.

Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009.

4.2.3. Some important Definitions

(a) “Communication” means dissemination, transmission, carriage of information or signal in some manner and include both a direct communication and an indirect communication”;

(b) “communication link” means the use of satellite, microwave, radio, terrestrial line, wire, wireless or any other communication media to inter-connect computer resource;

(c) “Competent authority” means--

(i) The Secretary in the Ministry of Home Affairs, in case of the Central Government; or

(ii) the Secretary in charge of the Home Department, in case of a State Government or Union territory, as the case may be;

(d) “Computer resource” means computer resource as defined in clause (k) of sub-section (1) of section 2 of the Act;

(e) “Decryption” means the process of conversion of information in non-intelligible form to an intelligible form via a mathematical formula, code, password or algorithm or a combination thereof;

(f) “Decryption assistance” means any assistance to--

(i) Allow access, to the extent possible, to encrypted information; or

(ii) Facilitate conversion of encrypted information into an intelligible form;

(g) “Decryption direction” means a direction issued under Rule (3) in which a decryption key holder is directed to--

(i) Disclose a decryption key; or

(ii) Provide decryption assistance in respect of encrypted information

(h) “Decryption key” means any key, mathematical formula, code, password, algorithm or any other data which is used to--

(i) Allow access to encrypted information; or

(ii) Facilitate the conversion of encrypted information into an intelligible form;

(i) “decryption key holder” means any person who deploys the decryption mechanism and who is in possession of a decryption key for purposes of subsequent decryption of encrypted information relating to direct or indirect communications;

4.2.4. Direction for interception or monitoring or decryption of any information:

No person shall carry out the interception or monitoring or decryption of any information generated, transmitted, received or stored in any computer resource under sub-section (2) of section 69 of the Act, except by an order issued by the competent authority;

Provided that in unavoidable circumstances, such order may be issued by an officer, not below the rank of Joint Secretary of the Government of India, who has been duly authorized by the competent authority;

Provided further that in a case of emergency--

(i) In remote areas, where obtaining of prior directions for interception or monitoring or decryption of information is not feasible; or

(ii) for operational reasons, where obtaining of prior directions for interception or monitoring or decryption of any information generation, transmitted, received or stored in any computer resource is not feasible,

the interception or monitoring or decryption of any information generated, transmitted, received or stored in any computer resource may be carried out with the prior approval of the Head or the second senior most officer of the security and law enforcement agency (hereinafter referred to as the said security agency) at the Central level and the officer authorised in this behalf, not below the rank of the Inspector General of Police or an officer of equivalent rank, at the State or Union territory level;

Provided also that the officer, who approved such interception or monitoring or decryption of information in case of emergency, shall inform in writing to the competent authority about the emergency and of such interception or monitoring or decryption within three working days and obtain the approval of the competent authority thereon within a period of seven working days and if the approval of competent authority is not obtained within the said period of seven working days, such interception or monitoring or decryption shall cease and the information shall not be intercepted or monitored or decrypted thereafter without the prior approval of the competent authority.

4.2.5. Authorisation of agency of Government:

The competent authority may authorize an agency of the Government to intercept, monitor or decrypt information generated, transmitted received or stored in any computer resource for the purpose specified in sub-section (1) of section 69 of the Act.

4.2.6. Issue of decryption direction by competent authority:

The competent authority may, under Rule (3), give any decryption direction to the decryption key holder for decryption of any information involving a computer resource or part thereof.

4.2.7. Interception or monitoring or decryption of information by a State beyond its jurisdiction

Notwithstanding anything contained in Rule (3), if a State Government or Union territory Administration requires any interception or monitoring or decryption of information beyond its territorial jurisdiction, the Secretary in-charge of the Home Department in that State or Union territory, as the case may be, shall make a request to the Secretary in the Ministry of Home Affairs, Government of India for issuing direction to the appropriate authority for such interception or monitoring or decryption of information

4.2.8. How to seek information from a mobile service provider?

Information from mobile service provider can be requested with the help of a 91 / 92 Cr.P.C. notice with a respective phone number or IMEI number. The service provider will respond with a Call Detail Record (CDR) if it is available in his network. The service provider will unable to handover CDR if the suspect has opted for Mobile Number Portability (MNP).

4.3. CALL DETAIL RECORD (CDR)

A Call Data Record (CDR) is a detailed record of SMS and calls that are sent and received by a subscriber of a service provider. It provides a wealth of information which can help in identifying suspect's day location, night location, handset details, maximum contacted number, date, time, tower location etc.,

Fig: Mobile Service Providers

The following details can be obtained from the MSP

- Call Detail Record (CDR)
- Subscriber Detail Record (SDR)
- Customer Application form (CAF)

4.3.1. CDR formats

- Text (plain text)
- Html (hypertext markup Lang)
- .xls (Excel file format)
- .csv (comma-separated value)- flat file
- .pdf (portable document format)

The formats mentioned above are very inconsistent as no service provider has a guideline on which format has to be given to the requestor. All these formats are auto-generated by the systems at service providers and can be emailed by the nodal agency /officer of that particular Mobile Service Provider (MSP).

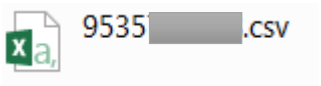
There are many investigation data sources that can be obtained from the service provider like:

- Cell phone details
- Tower info (TDR)
- Landline call details
- International call details (call route through a gateway)
- Subscriber details
- Cell phone forensic tools
- SIM card data extraction
- Telephone interception records

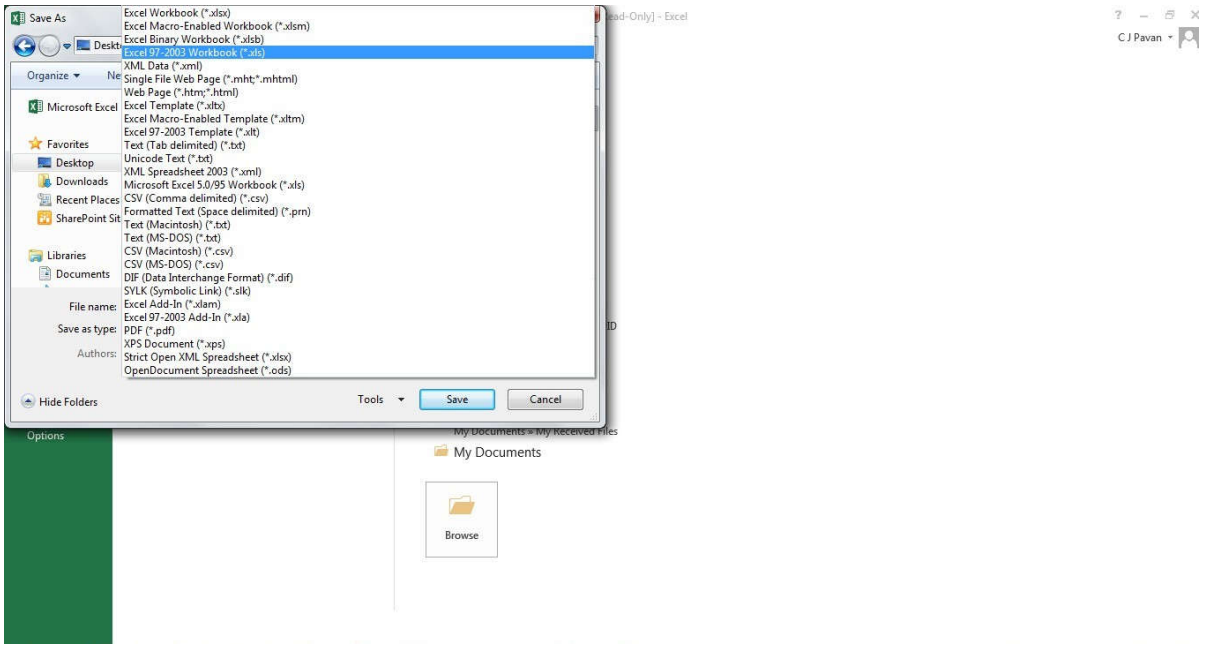
4.3.2. CDR Analysis

The following are the steps to perform a basic CDR analysis using MS-excel. The CDR obtained from the service provider is in the CSV format.

Step1: Open the CSV file in MS-excel



Step 2: Convert the .CSV file to .XLS file for analysis using save as option.



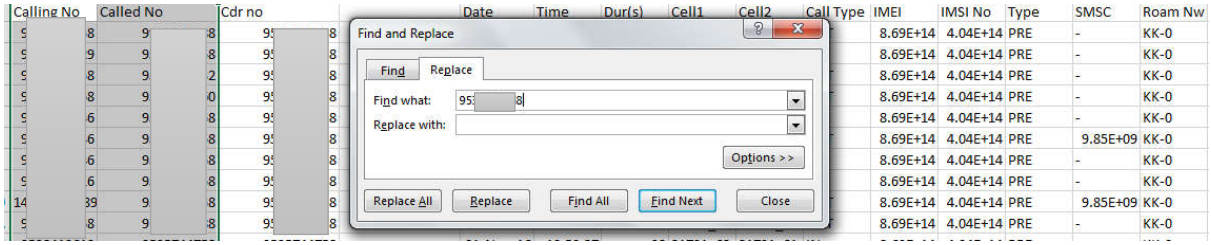
Step 3: Remove merged cells or additional cells (Detailing service provider, needs no signature etc.)

Calling No	Called No	Date	Time	Dur(s)	Cell1	Cell2	Call Type	IMEI	IMSI No	Type	SMSC	Roam Nw
[redacted]	[redacted]	01-Nov-16	00:09:58	45	21791_634	21791_634	OUT	8.69E+14	4.04E+14	PRE	-	KK-0
[redacted]	[redacted]	01-Nov-16	08:32:41	45	21791_634	21791_634	IN	8.69E+14	4.04E+14	PRE	-	KK-0
[redacted]	[redacted]	01-Nov-16	09:10:21	20	21791_634	21791_634	OUT	8.69E+14	4.04E+14	PRE	-	KK-0
[redacted]	[redacted]	01-Nov-16	09:11:24	180	21791_634	21791_634	OUT	8.69E+14	4.04E+14	PRE	-	KK-0
[redacted]	[redacted]	01-Nov-16	10:30:20	70	21791_307	21791_307	IN	8.69E+14	4.04E+14	PRE	-	KK-0
[redacted]	[redacted]	01-Nov-16	10:32:49	0	21791_634	-	SMT	8.69E+14	4.04E+14	PRE	9.85E+09	KK-0
[redacted]	[redacted]	01-Nov-16	10:37:29	9	21791_634	21791_634	IN	8.69E+14	4.04E+14	PRE	-	KK-0

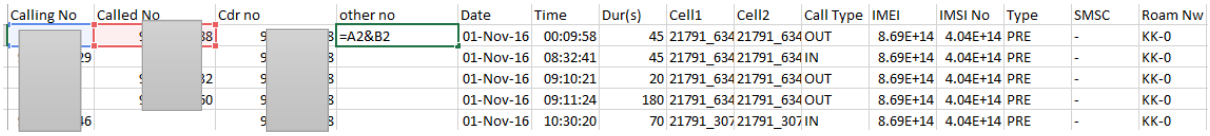
Step 4: Insert two columns after Calling No, Called No (Column c & column D) and copy CDR number in column C and leave the column D empty you can mention CDR no as heading in column C and Other no as heading in Colum D as shown below

Calling No	Called No	Cdr no	other no	Date	Time	Dur(s)	Cell1	Cell2	Call Type	IMEI	IMSI No	Type	SMSC	Roam Nw
[redacted]	[redacted]	[redacted]		01-Nov-16	00:09:58	45	21791_634	21791_634	OUT	8.69E+14	4.04E+14	PRE	-	KK-0
[redacted]	[redacted]	[redacted]		01-Nov-16	08:32:41	45	21791_634	21791_634	IN	8.69E+14	4.04E+14	PRE	-	KK-0
[redacted]	[redacted]	[redacted]		01-Nov-16	09:10:21	20	21791_634	21791_634	OUT	8.69E+14	4.04E+14	PRE	-	KK-0
[redacted]	[redacted]	[redacted]		01-Nov-16	09:11:24	180	21791_634	21791_634	OUT	8.69E+14	4.04E+14	PRE	-	KK-0
[redacted]	[redacted]	[redacted]		01-Nov-16	10:30:20	70	21791_307	21791_307	IN	8.69E+14	4.04E+14	PRE	-	KK-0

Step 5: Select Calling No and Called No (Column A & column B) and press control and H key simultaneously. Copy the CDR number in Find what field and replace with Space.

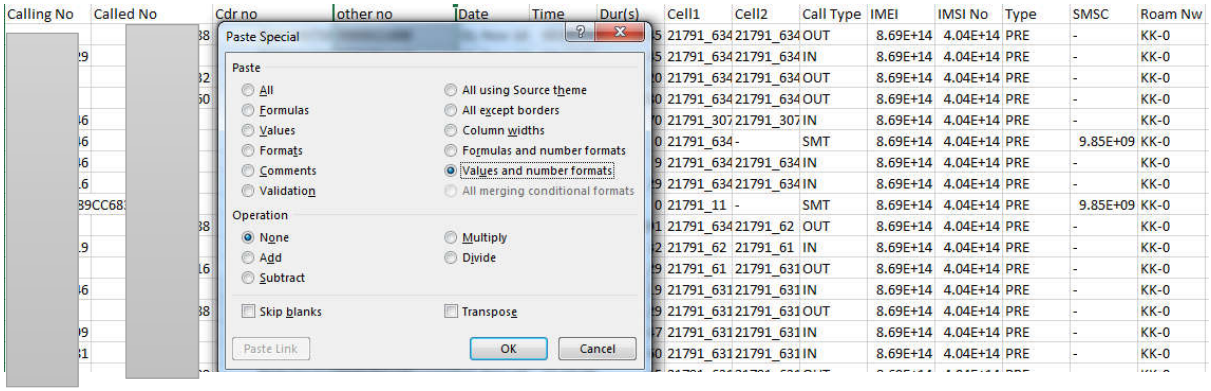


Step 6: In column D or Other No use this formula (=a2&b2) and press enter. Double-clicking on the edge of the green box inserts the number to all the columns till the end of the CDR.

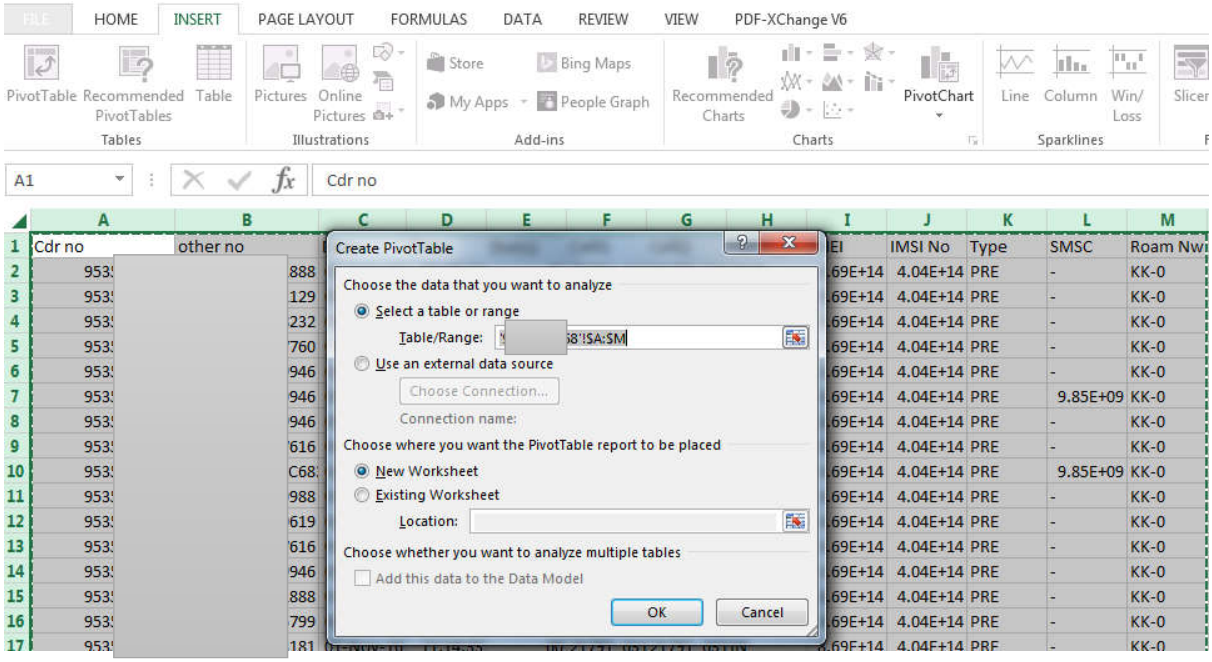


Calling No	Called No	Cdr no	other no	Date	Time	Dur(s)	Cell1	Cell2	Call Type	IMEI	IMSI No	Type	SMSC	Roam Nw
[redacted]	[redacted]	[redacted]	=A2&B2	01-Nov-16	00:09:58	45	21791_634	21791_634	OUT	8.69E+14	4.04E+14	PRE	-	KK-0
				01-Nov-16	08:32:41	45	21791_634	21791_634	IN	8.69E+14	4.04E+14	PRE	-	KK-0
				01-Nov-16	09:10:21	20	21791_634	21791_634	OUT	8.69E+14	4.04E+14	PRE	-	KK-0
				01-Nov-16	09:11:24	180	21791_634	21791_634	OUT	8.69E+14	4.04E+14	PRE	-	KK-0
				01-Nov-16	10:30:20	70	21791_307	21791_307	IN	8.69E+14	4.04E+14	PRE	-	KK-0

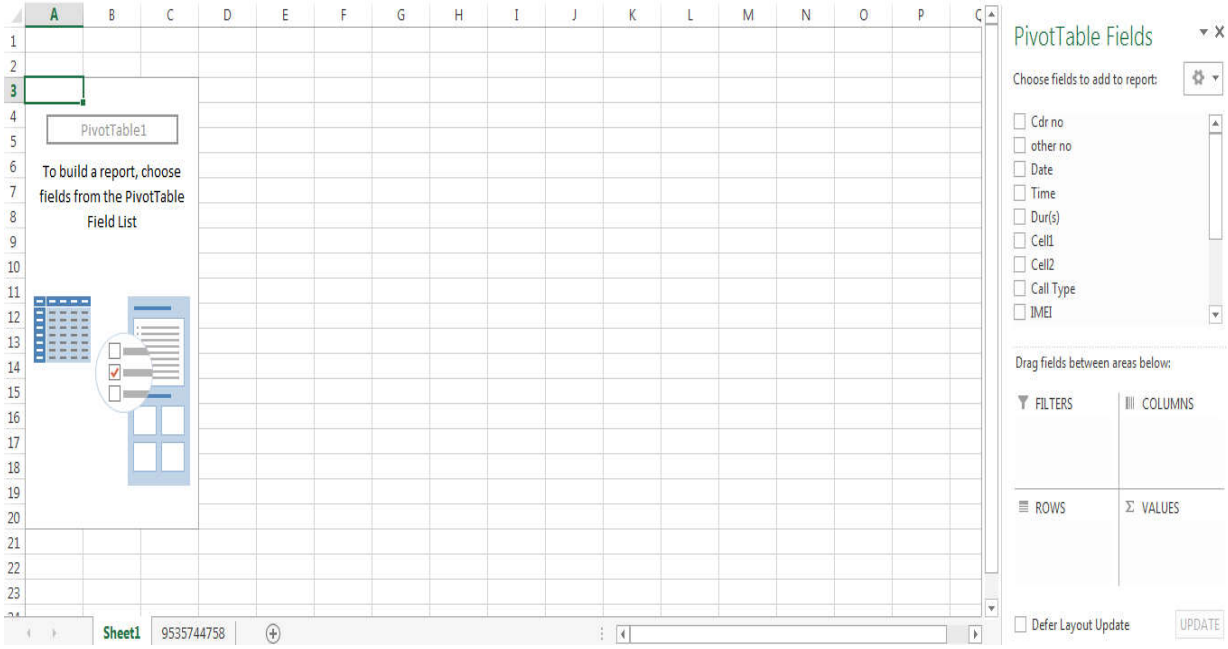
Step 7: Right click on column D and copy the entire column and again right click on the same column you will get an option of paste special. Select paste special and select values and number formats as shown in the below fig



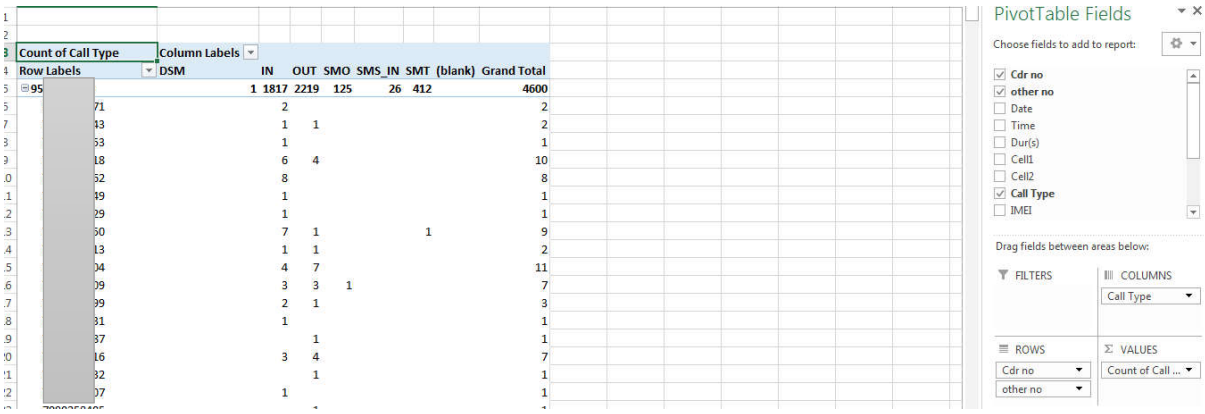
Step 8: Select the entire sheet and select insert option and click on the pivot table and the following option shown below appears. Click ok.



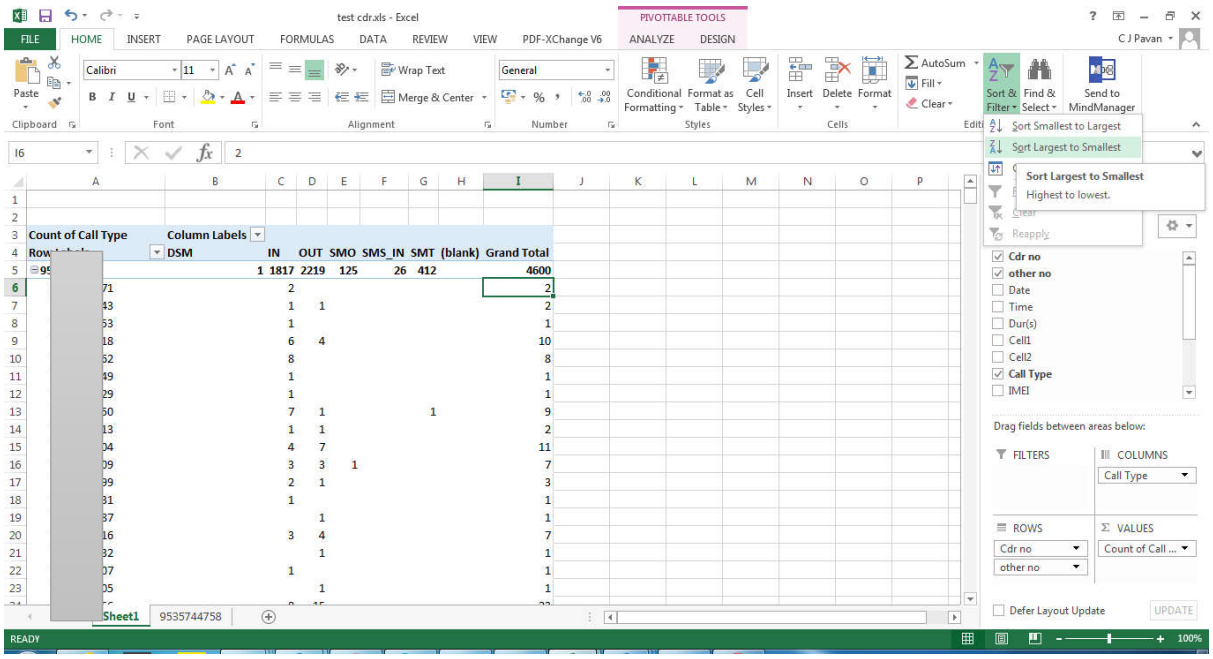
Step 9: The following sheet will open in your xls sheet.



Step 10: select CDR no and other number, Drag and drop both numbers on Rows. Select call type and drag and drop on values, Select call type again and drag and drop in column



Step 11: Select any number in the last column (In the below fig "2" is selected) click on home and select sort Largest to Smallest



Count of Call Type	Column Labels							
Row Labels	DSM	IN	OUT	SMO	SMS_IN	SMT	(blank)	Grand Total
95[redacted]		1	1817	2219	125	26	412	4600
[redacted]71			2					2
[redacted]43			1	1				2
[redacted]53			1					1
[redacted]18			6	4				10
[redacted]62			8					8
[redacted]49			1					1
[redacted]29			1					1
[redacted]50			7	1			1	9
[redacted]13			1	1				2
[redacted]04			4	7				11
[redacted]09			3	3	1			7
[redacted]99			2	1				3
[redacted]31			1					1
[redacted]87				1				1
[redacted]16			3	4				7
[redacted]32				1				1
[redacted]07			1					1
[redacted]05				1				1

Step 12: The following is the maximum contacted numbers to the CDR number.

Count of Call Type		Call Type							
Cdr No	Other No	DSM	IN	OUT	SMO	SMS_IN	SMT	(blank)	Grand Total
95[redacted]3	95[redacted]0		34	213	4	1	3		255
	94[redacted]9		58	112	3		1		174
	73[redacted]1		57	56			1		114
	96[redacted]6		58	47	1		5		111

4.4. Other Mobile related investigations

4.4.1. Role of Tower dump analysis in investigations

It is a very important tool of investigation in cases where there is no suspect for a crime and only a few peripheral details are available with the crime investigation agency.

The precise reason for any tower dump analysis is to find out the unknown suspects. In short, tower dump is the CDR of a tower.

E.g. A major theft of gold worth Rs. 1 crore was reported from the jewelry owner. The CCTV footage was retrieved, however, faces of the suspects were covered.

4.4.2. Internet Protocol Detail Record (IPDR):

IPDR is the record of internet activities of mobile subscribers when they are assigned with an IP address when they are connected to the internet.

An IP data record can tell you a number of things about incoming and outgoing traffic like source and destination IP address, Ports, time of access

The below fig shows a sample of IPDR

PRIVATEIP	PRIVATEPORT	PUBLICIP	PUBLICPORT	DESTIP	DESTPORT	MSISDN	IMSI	START_DA	START_TI	END_DATE	END_TIME	IMEI	CELL_ID
10.1[redacted]	56614	1.[redacted]	43452	50.[redacted]	5222	9.19737E+11	4.06E+14	#########	04:11:47	########	19:27:11	3.52E+15	4.06E+15
10.2[redacted]	33073	1.3[redacted]	4267	216[redacted]	443	9.18377E+11	4.04E+14	#########	14:22:08	########	15:48:08	3.52E+15	4.04E+14
10.2[redacted]	33073	1.3[redacted]	4267	216[redacted]	443	9.18377E+11	4.04E+14	#########	14:22:08	########	16:04:10	3.52E+15	4.04E+14
10.2[redacted]	43764	1.3[redacted]	1539	31.1[redacted]	443	9.18586E+11	4.04E+14	#########	15:34:47	########	15:38:19	3.58E+15	4.04E+14
10.2[redacted]	43766	1.3[redacted]	55865	31.1[redacted]	443	9.18586E+11	4.04E+14	#########	15:34:47	########	15:38:19	3.58E+15	4.04E+14

4.4.3. Voice over IP (VOIP) based investigations

Voice over IP has made the communication easier and cheaper and with the introduction of lower fares for 3G/4G services, there has been a spurt in the number of mobile applications which make people capable of making voice calls using the data services.

Voice over IP (VOIP) technology enables the transfer of voice and multimedia content over Internet Protocol (IP) networks. In simple words, VoIP is basically a telephone connection over the Internet.

4.4.4. Investigation of VOIP

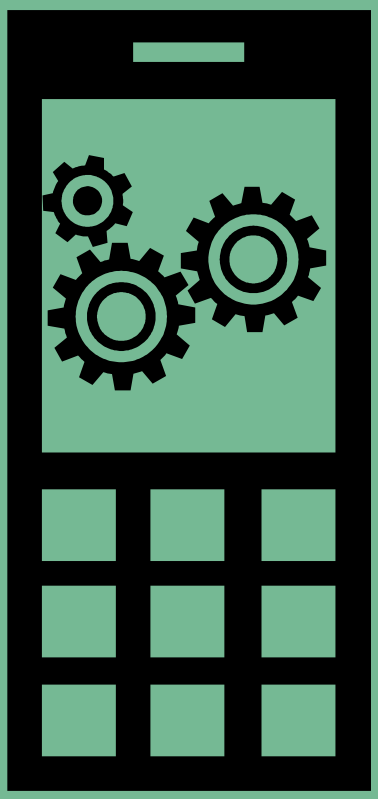
- Take the CDR of the victim from the service provider.
- Contact that respective service provider for Trunk Gateway (TG) details of the call.
- Upon receiving the details from trunk gateway identify the gateway from where such VoIP calls were originated e.g. Reliance, VSNL etc.,
- The gateway will furnish further details of VOIP carrier used to route the call which can be like Skype, Nymgo, etc
- Then the VOIP carrier will give us the registration and access details of the end user such as username, registered e-mail, created and last access IP address etc.,

4.5. Case study: Threating call over the internet

Cybercrime police station received a complaint from a complainant that he has received a threatening call on his mobile. The number displayed on complainant mobile was +177777.

- ✓ Cyber cell requested the CDR of a complainant's cell number of said period and the same number was found even in the CDR
- ✓ Cyber Cell asked mobile service provider to provide an incoming gateway of that particular call.
- ✓ Cyber Cell searched for the originating telecom company which was based out of India
- ✓ The company was contacted through e-mail from the cyber crime police station and the response was received from them having the following details
    - Name
    - Email
    - IP from where he created an account
    - Last Login
    - Phone Number

  The IP was traced outside India. However, e-mail logs were obtained from the email service provider and the IP address belonged to Indian service provider. A notice was sent under 91 CrPC to obtain the physical address of the IP and the suspect was arrested.



CHAPTER 5

Mobile Forensics

CHAPTER 5

Mobile Forensics

Why should you read this Chapter?

The goal of this chapter is to introduce you about mobile forensics and procedures to collect required evidences from mobile devices.

After reading this chapter, you would be:

- Able to understand about the evidences that can be extracted from a mobile device for the purpose of investigation.
- Know standard procedures about the seizure of devices from the scene of crime.

5. Introduction to mobile forensics

Internet and mobile phones are the most used technology in the world. The widespread of wireless telecommunication technology has touched every aspect of human life. Mobile technology enables users to communicate and access information or resources through the internet from anywhere, provided that network (signal) is available.

The penetration of smartphones in our daily lives has enabled communication as well as other cyber and network related works such as banking, shopping, paying bills, booking travel tickets etc. However, it has also provided easy avenues to commit cyber-frauds leading to increase in forensic cases.

A mobile phones stores a wide array of personal data such as pictures, images, videos, call logs, SMS, e-mails and data pertaining to various applications installed etc. Along with digital data, mobile phone devices can also be used for the collection of other evidence like ear prints, sweat, saliva and fingerprints that can be used in the investigation to find any association between crime and the criminal. The present chapter presents a systematic process of collection of evidence from the crime scene and its investigation.

5.1. Major mobile phone related Cyber Crimes

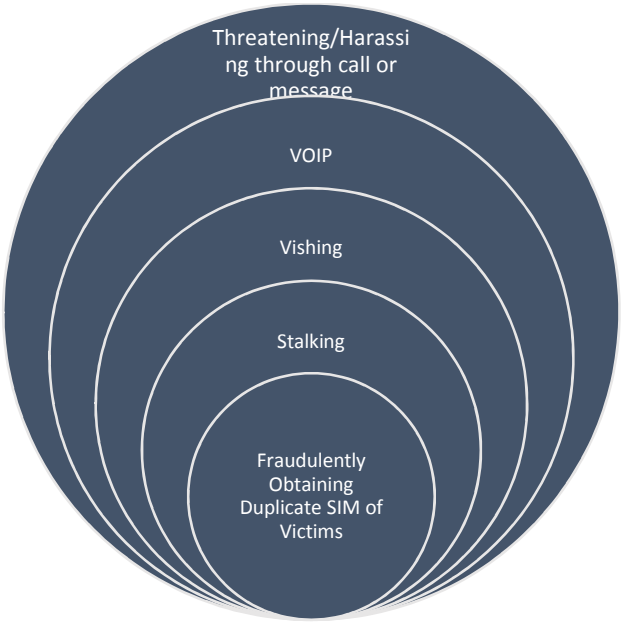


Fig: Mobile related crimes

5.2. Mobile Forensics definitions

Definition 1: Mobile phone forensics is the science of recovering digital evidence from a mobile phone under forensically sound conditions using accepted methods.[9]

Definition 2: Mobile phone forensics is the utilization of scientific methodologies to recover data stored by a mobile phone for legal purposes[10]

5.2.1. Evidence in Mobile Devices

Mobile phone has the similar potential of holding evidence as any other digital media.

5.2.2. Evidence that can be extracted from a traditional mobile device:

- Hardware
    - Handset make, Model, Serial Number
    - International Mobile Equipment Identity (IMEI)
- User-created evidence
    - Address book
    - Message logs (SMS, MMS) – sent, received deleted
    - calendar
    - memos, to-do lists, notes
- Mobile Device created evidence
    - Call logs - Calls received, dialled numbers, missed calls, etc.
    - Deleted calls, service SMS etc.

5.2.3. Evidence that can be extracted from a smartphone:

- User Created evidence
    - Photographs (including EXIF metadata); video/audio; maps
    - MMS, GPS waypoints; stored voicemail
- Internet-related evidence
    - Online accounts; purchased media (often discoverable in embedded metadata)
    - Email content; Internet usage; social networking information, etc.
- Third party installed apps
    - Alternate messaging and communication systems; additional capabilities; malware applications; e-commerce applications etc.,
    - Chat Logs, spoofing apps, VPNs etc.

Note: Metadata is data about data. It describes and gives information about other data. E.g. file crated, modified and accessed date & time, metadata of photos (latitude, longitude, equipment make, camera model etc.)

[9] Guidelines on mobile device forensics ,Recommendations by NIST, Special Publication 800-101
[10] SWDGE Best Practices for Mobile Phone Forensics

5.2.4. Evidence related to the intermediaries (mobile service provider)

- CDR
- CAF
- IMEI
- IMSI
- Location
- PUK

5.3. Types of memory on mobile phones

1. Mobile Phone Internal Memory: it is also called as phone main memory or primary memory which has direct access with the processor in a mobile phone. Flash memory consisting of NAND or NOR types are used in mobile devices
2. Mobile Phone External Memory: it is also called as secondary memory, it is not directly accessed by the processor of the mobile phone but the processor uses the input/output channels to access the secondary memory. The size of the secondary memory depends on the support provided by the handset manufacturer. Few smartphone models support till 2TB of external memory
3. Subscriber identity module (SIM): It is a smart card that stores data for GSM cellular telephone subscribers. Such data includes user identity, location and phone number, network authorization data, personal security keys, contact lists and stored text messages.
4. Cloud storage: Users can store data on cloud storage as well. For e.g., Once a user registers with Gmail, the user is entitled to get 15GB free google drive space where the user can store pictures, video, synchronized data of WhatsApp etc.,

The pictorial representation of types of memory associated with a mobile phone is shown in the below fig

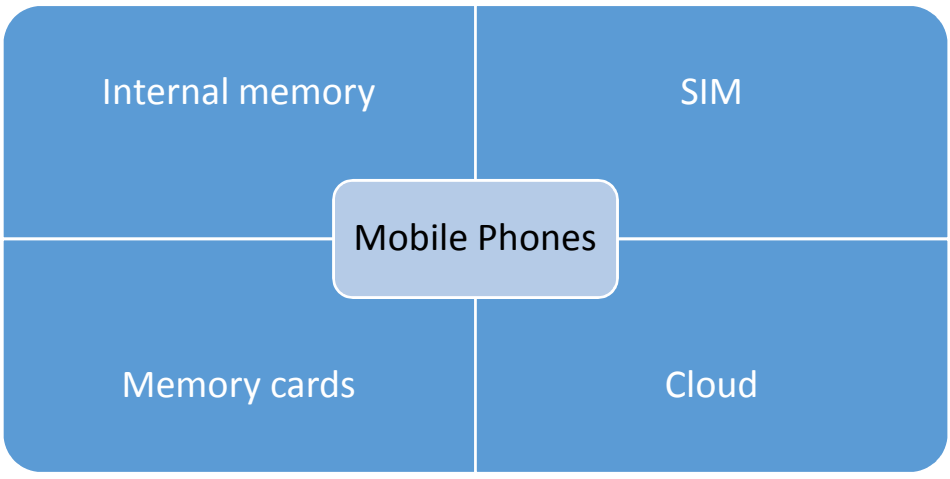


Fig: Types of mobile phone data storage

The table is given below shows different pieces of evidence stored and their locations[11]:

Evidence	Source
Name of the service provider	Printed on SIM.
Location area identity(LAI)	Stored inside SIM
Integrated circuit card identifier	Stored inside SIM and Some providers only print abbreviated version on card
International Mobile Subscriber Identity (IMSI)	Stored inside SIM and it is unique id for every subscriber
Text Messages Data (SMS)	Stored on SIM as well as on handset
contacts	Stored on SIM as well as on handset
Call logs	Stored on SIM as well as on handset
International Mobile Equipment Identity (IMEI)	Stored as well as printed on Mobile
Multimedia Messages	Mobile phone memory/ External memory
images/Sound/Videos	Mobile phone memory
WAP/Browser History/Emails	Mobile phone memory
Calendar Items / Notes	Mobile phone memory
Information on Previous SIMs	Few mobile phones also hold information on previously used SIM cards
MSISDN (Mobile Subscriber Integrated Services Digital Network) / Telephone Number.	At times available in SIM memory. Few network operators give facility to dial some code for finding it
App data/Mail/Synced data	Cloud

Note: The forensic copies of the SIM card and memory cards can be created using a card reader. A significant amount of deleted data like Photos, videos, text files, etc. can be recovered from memory cards. They can be analysed using established forensic tools like Encase, FTK, etc. meant for computer forensics.

5.4. Techniques of Mobile Forensics

Forensic tools acquire data from a device in one or two ways: physical acquisition or logical acquisition.

Physical acquisition implies a bit-by-bit copy of an entire physical store (e.g., a memory card, internal memory, SIM card)

Logical acquisition implies a bit-by-bit copy of logical storage objects (e.g., directories and files) that reside on a logical store (e.g., a file system partition). The difference lies in the distinction between memory as seen by a process through the operating system facilities (i.e., a logical view), versus memory as seen in raw form by the processor and other related hardware components (i.e., a physical view).

Physical acquisition has advantages over logical acquisition, since it allows deleted files and any data remnants present (e.g., in unallocated memory or file system space(*.mp3,mp4,3gp,mov,jpg etc.) to be examined, which otherwise would go unaccounted.

[11] Mobile Phone Forensics Challenges, Analysis and Tools Classification by Amjad Zareen, Dr Shamim Baig.

Methods of extracting data

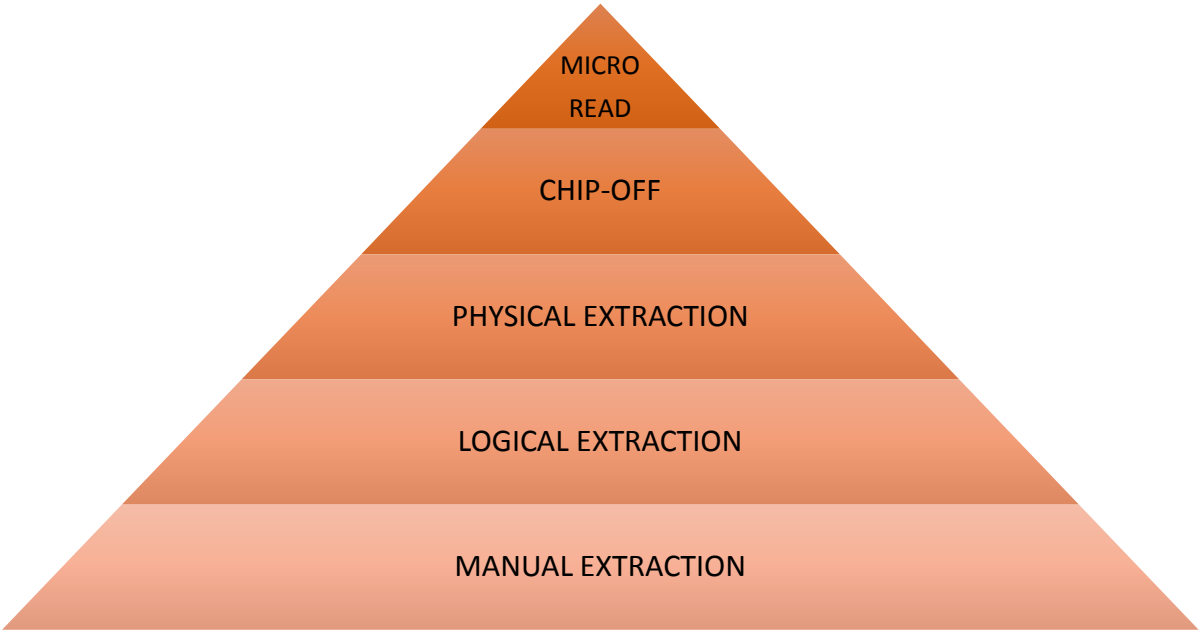


Fig: Mobile data extraction methods

Based on the various extraction methods, each existing mobile forensic tool can be classified under one of the five levels:

Manual Extraction: A manual extraction method involves viewing the data content stored on a mobile device. The content displayed on the screen requires the manual manipulation of the buttons, keyboard or touchscreen to view the contents of the mobile device. Information discovered may be recorded using an external digital camera. At this level, it is impossible to recover deleted information. Some tools have been developed to provide the forensic examiner with the ability to document and categorize the information recorded more quickly.

Logical Extraction: Connectivity between a mobile device and the forensics workstation is achieved with a connection using either a wired (e.g., USB) or wireless (e.g., IrDA, Wi-Fi, or Bluetooth) connection. The examiner should be aware of the issues associated when selecting a specific connectivity method, as different connection types and associated protocols may result in data being modified or different types of data being extracted. Logical extraction tools begin by sending a series of commands over the established interface from the computer to the mobile device. The mobile device responds based upon the command request. The response (mobile device data) is sent back to the workstation and presented to the forensics examiner for reporting purposes.

Physical extraction: In this method bit by bit image is created called hex dump. A piece of code (or agent) is copied to the memory of the mobile phone from the forensic software's and execute commands to automatically collect the user data and store it on the destination location selected by the examiner. Many tools are capable of extracting data from the image and generate a report in the format specified by the user who can do further analysis easily.

Chip-Off: This methods refer to the acquisition of data directly from a mobile device's flash memory. This extraction requires the physical removal of flash memory. Chip-Off provides examiners with the ability to create a binary image of the removed chip. In order to provide the examiner with data in a contiguous binary format file, the wear-levelling algorithm must be reverse engineered. Once complete, the binary image may then be analyzed. This type of acquisition is most closely related to physical imaging a hard disk drive as in traditional digital

forensics. Extensive training is required in order to successfully perform extractions at this level.

Micro Read: This process involves manually viewing and interpreting data which is seen on a memory chip/phone using a high power microscope. The process is time consuming, costly and requires extensive knowledge of all aspects of Flash memory and the file system.

5.5. List of Mobile Forensics Tools

Sl. No	Item	Purpose
1	Cellebrite UFED 4PC with Chinex	Standalone mobile forensic extraction device and software's that combines multiple mobile device support with universal data extraction technology to perform physical, file system and logical extractions of all data from the widest range of mobile devices.
2	Oxygen Forensics Detective	
3	MOBILedit Forensic express	
4	Elcomsoft iOS Forensic Toolkit/ Elcomsoft Phone Breaker	
5	XRY Physical/Logical	
6	MOBILedit Forensic	
7	Paraben's Device Seizure	
8	Access Data MPE+	
9	Logicube CellXtract	
10	Berla Blackthorn	GPS forensics

5.6. Challenges in extraction of Forensic evidence from communication devices:

Mobile forensics is dynamic in nature, where there are no standards and every device is proprietary with different operating systems. As phones tend to have embedded operating systems, generally you have to turn them on to recover the data, which is not the same as computer forensics or disk forensics. We only grab what the tools easily find with the help of sophisticated tools. We are adapting ourselves to the role of technician and not doing any analysis.

The challenges will grow as the technology advances day by day.

- Getting smaller and using complex hardware.
- Huge diversity of Operating systems.
- No standard protocol for data extraction.
- Encryption
- Different Data Cables and Data Communication Ports
- Made in China Phones
- Cloud storage

5.7. Investigative Procedures

Investigative methods are procedures the investigative team can apply, which require no forensic software or hardware tools. The most obvious methods are the following:

- **Ask the owner** – If a device is protected with a password, PIN or other authentication mechanism involving knowledge-based authentication, the owner may be queried for this information during an investigation.

- **Know the service provider** – Unstructured Supplementary Service Data (USSD) sometimes referred as short codes can be used by dialing these codes on the mobile phones of suspects and victims to find out their mobile numbers.

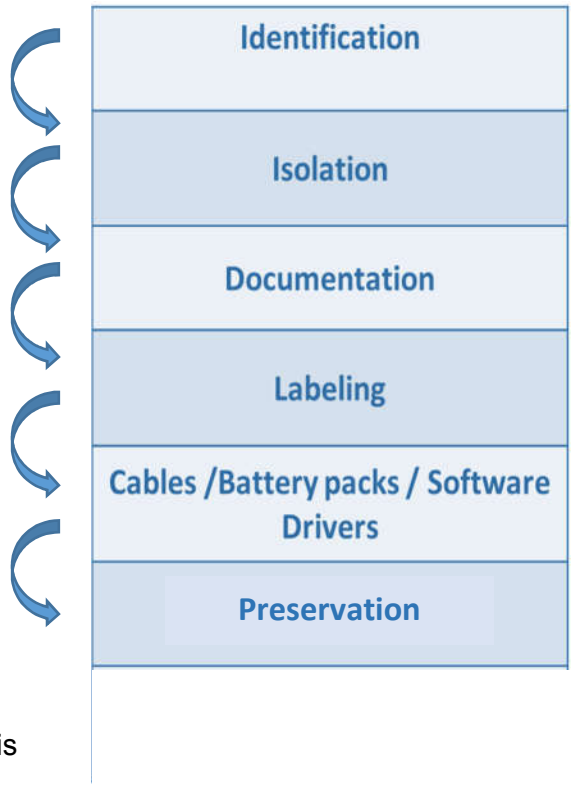
  Some indicative codes are listed below

Service provider	code
Airtel	• *121*1# or *121*9#
Vodafone	• *111*2#
Idea	• *131*1#
BSNL	• *222# OR *888# OR *1# OR *785# OR *555#
Reliance mobile	• *1#

- **Mobile forensic Process--** The mobile forensics process aims to recover digital evidence or relevant data from a mobile device in a way that will preserve the evidence in a forensically sound condition

5.8. Steps involved in the analysis of mobile devices:

1. **Identification** is the process of identifying the mobile device in scene of crime or through IMEI lookup in CDR.
2. **Isolation** of mobile device from external communication is very important to avoid further logging of calls and messages after seizure which may lead to loss of critical evidence.
3. **Documentation** of each and every aspect of procedures followed in seizure of mobile is also very important.
4. **Labelling:** It's very important to **label** the number of devices, memory cards, SIM cards mobile phone cover, if any and other relative accessories while seizure.
5. It is a best practice to charge the battery to its full capacity before sending it to the forensic examination. The forensic experts can directly start acquisition of mobiles without charging the phones making the analysis of devices less time consuming.
6. **Preservation** without changing the data integrity is also very important in after acquisition.



5.9. Precautions to be taken before an investigation

1. Occasionally, there may be a need to conduct traditional forensic processes on a mobile phone (e.g., DNA and latent prints).
2. Isolate the mobile device by switching off the phone or use the flight mode option if available.
3. Take photos of the crime scene which include cell phones, wires, connectors, etc.
4. Search for papers, sticky-notes, diaries and any other evidence which may give out passwords or other vital information.
5. Label all the wires, connectors and devices and bag them with evidence.
6. Make sure to maintain proper chain of custody details for each evidence items seized.

5.10. Scenario: If a mobile device is recovered from a bomb blast site

1. Use hand gloves or other clean sterile cotton cloth while recovering the mobile device from the scene of the crime.
2. Use the plastic envelope to hold the evidence.
3. Send the phones to FSL and CFSL for recovering physical (e.g. finger prints, DNA) and digital evidence (e.g. call logs, SMS etc.) associated with the phone

Note: Law enforcement may seek assistance or consult with the forensic experts for gathering/recovering traditional evidences like DNA, Fingerprint etc. and digital evidences like phones, pen drives, laptops, desktops, external hard disk drives etc.,

5.10.1. If Cell Phone is Switched On

If the phone is in on condition, keep the device isolated by selecting flight mode option**.** If the flight mode option is not available use the faraday bag (faraday bag helps to block any kind of external electromagnetic signals which might affect the data in the communication de vices) to isolate the phone. Mobile device should be plugged to a power bank so that the device does not switch off. If the faraday bag is also not available wrap the mobile in aluminium foil.

If the mobile device is synced to a computer or laptop and data transfer is occurring, do not pull the phone away from the computer / laptop as data in transfer will be lost.

Further, the device should be sent by fastest mode to forensic examiner in switched-on condition.

5.10.2. If Cell Phone is OFF

- Remove Battery and Take a photo of the position of SIM(s)
- Pack Battery, SIM, and Handset separately.
- Note Down the details of SIM and Handsets like *Make, Model, IMEI, ICCID* etc.
- If the phone is immersed in a liquid, take the phone out, remove battery, SIM card(s) & also, collect a small quantity of the liquid in which phone was immersed to prove the effect of the liquid on the present state of the phone

The below fig determines indicative flow for acquiring evidence from mobile devices

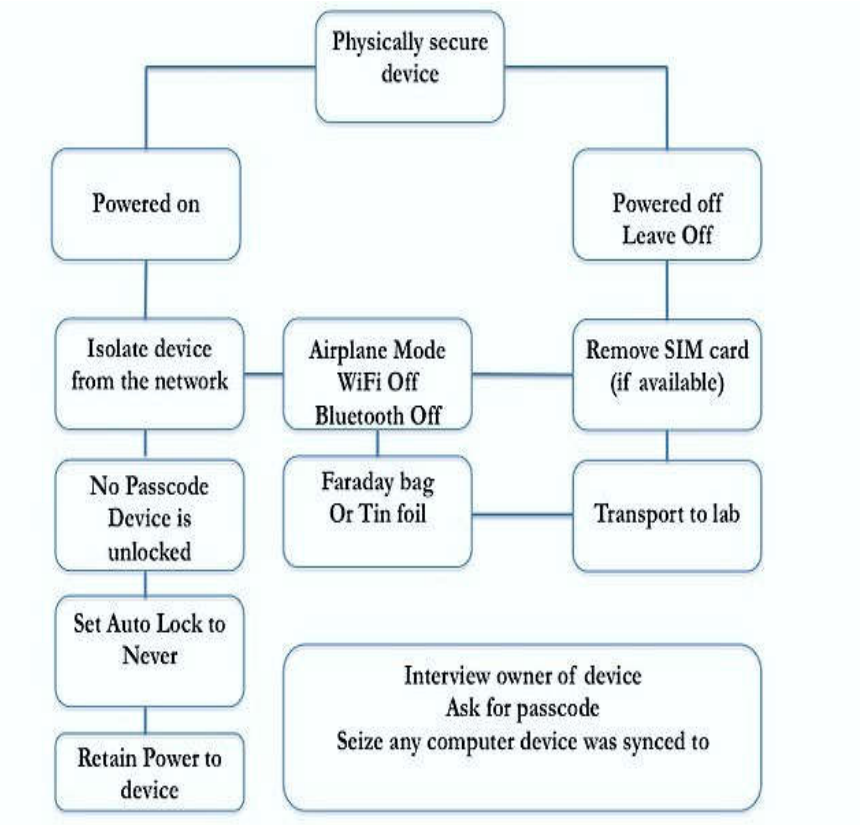


Figure: acquisition of mobile phone

CHAPTER 6

Investigation of Financial Frauds & cyber crimes

CHAPTER 6

Investigation of Financial Frauds & cyber crimes

Why should you read this Chapter?

After reading this Chapter, you would be able to understand

- Investigation procedures related to financial frauds.
- Investigation procedures for common cyber-crimes, modus operandi etc.

6. Introduction to investigation of cybercrimes & financial frauds

The Internet is becoming ubiquitous and people continue to venture into cyberspace to conduct more of their professional activities online, this has created vast opportunities for cybercrime & financial frauds. Investigation approach for cybercrime investigation is different compared to traditional crimes due to various complexities. The challenge is to collect the required data in time and to co-relate with the suspect. This chapter discusses various procedures for investigating cybercrimes & financial frauds

6.1. Steps to Follow in case of a fraudulent online transaction

1. Collect the bank statement from the concerned bank and identify the fraudulent transactions happened in the statement with the date and time.
2. Request the bank to provide the complete details of fraudulent transactions.

6.2. Investigation of ATM withdrawal cases

1. Identify the ATM Location in consultation with the bank.
2. Request for ATM CCTV footage & external CCTV Footages from the bank. Identify other CCTV cameras (If available) in the vicinity of the ATM and collect the same.

6.3. Investigation of online transaction cases

1. Collect the details of a merchant from the bank and merchant account details.
2. In cases of an e-commerce transaction, contact the e-commerce platforms like flipkart, Amazon, Snapdeal etc., and collect the delivery address, transaction IP, mobile number etc.,
3. In case of wallet transfer, contact the service provider and get the Know your Customer (KYC) details, mobile number, transaction details, and beneficiary details if the money is transferred to a bank account.

6.4. Investigation of Bank to Bank transfer

Collect the beneficiary account details to which the funds were transferred and also request account access IP Logs. Once you receive IP address perform WHOIS lookup of the IP to identify the service provider and issue a notice under 91CrPC to obtain the physical address.

6.5. Investigation transactions involving Cheques

1. Collect the copy of the cheque from the Bank and enquire in which bank was the cheques withdrawn and collect the CCTV Footage of the same to identify the person who has withdrawn the money using the cheque.
2. If the Cheque has been transferred to another account via normal cheque processing then collect the beneficiary bank account details.

6.6. Summary of common investigation steps

1. Take the CDR and SDR of mobile numbers associated with the concerned bank account(s).
2. Collect CAF(s) & KYC(s) from Mobile Service Providers (MSP) & Banks
3. Sometimes mobile numbers present in KYC of the bank is different than the registered mobile number for SMS alert. In such cases, collect the CDR, SDR & CAF of the same.

6.7. Indicative notice under 91 CrPC issued to the bank

POLICE NOTICE

(Under section 91 of Code of Criminal Procedure 1973)

To,

Sir/Madam,

Sub: Request to provide details with respect to *** bank
Credit /Debit card/ Account/ No:
Ref: (name of police station e.g. Ashok nagar, JP Nagar) Police Station CR No *******

*****

Brief facts about the case

Sample details requested from the bank

1. Account details from dd-mm-yy to dd-mm-yy
2. Access logs of the suspected account
3. Transaction details of debit/credit cards
4. CCTV clippings of ATM cameras from dd-mm-yy to dd-mm-yy

Yours truly,

(Signature, Name of IO & seal)

6.8. Key Definitions

1. **Customer ID and account number:** These are unique numbers that belong to you. A single ID is assigned to you even if you hold more than one account with the bank. However, each account will have a different account number.
2. **Account type:** Whether it is a savings or a current account.
3. **Account status:** Actively-operated accounts are marked 'Regular'. No transaction for six months makes them dormant. To re-activate or make a transaction, the branch has to be contacted.
4. **Nomination:** The beneficiaries of your account, especially if held by a single person, are mentioned at the start of the statement. It is important to have a beneficiary as it is difficult to make claims in case of a mishap or the account holder's death.

6.9. Key Abbreviations

- **IFSC**: *Indian Financial System Code*
- **NEFT**: National Electronic Fund Transfer
- **RTGS**: Real-time Gross Settlement Systems
- **IMPS**: Immediate Payment Service
- **MICR:** Magnetic Ink Character Recognition
- **IB, INF, NEFT, TPT:** some banks use the terms 'IB' (internet banking) fund transfer and 'INF' (internet fund transfer). 'NEFT' (National Electronic Funds Transfer) to transfer between two banks and 'TPT' in case of a third party transfer
- **ATW (NWB/VAT/MAT/NFS):** ATM withdrawals. When withdrawals occur at another bank's ATM, a few more abbreviations are added (as shown in the bracket)
- **VMT:** Visa money transfer through ATM
- **MMT:** MasterCard money transfer through ATM

6.10. Wallet transfers

In case of wallet money transfers. Contact the nodal officers of the wallet service providers & obtain registered mobile numbers, IP logs and KYC details, transaction details from them.

- ✓ If the money is deposited to bank, collect the beneficiary details.
- ✓ In case of e-commerce transaction. Identify the service provider and obtain the account details of the recipient.

6.11. Advance fee fraud

It is when fraudsters target victims to make *advance* or *upfront* payments for goods, services and/or financial gains that do not materialize. They deceive victims to deposit money as processing fee or transfer charges or charges for their services etc.

- Lottery frauds
- Job Frauds
- Matrimonial Frauds
- Loan Frauds etc.,

6.12. Lottery frauds

It is type of advance-fee fraud which begins with an unexpected email notification, phone call or mailing list.

Investigation of Lottery frauds:

- In case of SMS, its content and phone number to be collected and CDR should be analyzed & Customer Application Form (CAF)/Subscriber Detail Record (SDR) should be collected.
- In case of email, senders e-mail ID along with the header should be collected.
- If victim deposited the money, collect list of bank accounts to which money is paid and freeze the account, collect KYC forms, Phone numbers associated with that account.

6.13. Job Frauds

Fraudsters create numerous attractive schemes like easy hire in MNC, high salary etc.

Investigation of job frauds:

- Fraudsters may have opened fake/Impersonating website to lure victims. In this case collect website URL (e.g. www.xyz.com), search where the domain is hosted by looking up in Whois and collect the details of the person hosting the website by issuing notice under 91 CrPC to the registrar (web space provider/reseller)
- Fraudsters may send spoof emails to candidates. In this case, collect full e-mail header, analyze the header for originating IP
- Fraudsters may ask you to deposits through various bank accounts before/ on receiving fake offer letter. In this case, collect list of bank accounts to which money is paid and freeze the account, collect KYC forms, Phone numbers associated with that account.
- Fraudsters post online classifieds informing about the Job openings, Identify the **Ad id** and obtain the logs from the classified forums (e.g. quicker, OLX, locanto etc.,) Obtain the physical address of the IP address that you had received from the classified forum(s).

6.14. Matrimonial Frauds

Fraudsters create fake profiles on leading matrimonial websites for cheating.

Investigation of loan frauds:

- Collect the user profile URL from the victim and obtain registration details like phone numbers, mode of payment registration IP and access IP details of the fake profile
- Obtain Physical address of the IP address by issuing notice under 91 CrPC.
- Obtain CDR, SDR,CAF for mobile numbers
- If victim transfer the money to the bank, collect list of bank accounts to which money is paid and freeze the account, collect KYC forms, Phone numbers associated with that account

6.15. Loan Frauds

Scammers are skilled at convincing people that their loan offer is real by communicating e-mail, classifieds online and on newspapers etc., They make fake schemes that is willing to fund without any apparent due diligence.

Investigation of loan frauds:

- Fraudsters may ask you to deposits money upfront through various bank accounts as a loan processing fee, initial repayments etc., In this case, collect list of bank accounts to which money is paid and freeze the account, collect KYC forms, Phone numbers associated with that account

- Fraudsters post online classifieds about the loan offers, Identify the **Ad id** and obtain the logs from the classified forums (e.g. quicker, OLX, locanto etc.,) Obtain the physical address of the IP address that you had received from the classified forum(s).

Note: If you notice time as UTC in the IP logs. You have to convert the time from UTC to IST before asking for the physical address. You can use online time zone converter websites like http://www.timezoneconverter.com/cgi-bin/tzc.tzc to convert date and time to IST.

6.16. E-mail compromise frauds

The cyber criminals will identify and compromise corporate/business email account of individual who has the authority to perform fund transfers. It is expanding rapidly to the import and export business. They will compromise the account and monitor for the communication for financial transaction. Once they come to know the victim is going to receive funds they will impersonate themselves as victim company to the sender and mention reasons for change in bank account due to audit in the company, income tax etc., or they will create an e-mail id similar to the victim company. In such cases, following the money trail will help in identification of victims.

Investigation:

- Obtain the access logs of the account.
- Seek the details of beneficiary account from the complainant

The list of nodal officers of few service providers are mentioned in Annexure 3

CHAPTER 7

Investigation Abroad

CHAPTER 7

Investigation Abroad

Why should you read this Chapter?

After reading this Chapter, you would be able to understand

7. Important legal provisions for investigating abroad.
8. Guidelines for Investigation Abroad & Issue of Letters Rogatory (Lr)
9. Mutual legal assistance treaties

7. Introduction to investigation abroad

Internet and evolution of information technology have become a two edged sword, on one hand, several areas of social activity connected to everyday life, including, but not limited to, financial institutions, online business services, record keeping functions, interpersonal communications, and so on. On the other hand, it has also become attractive target for perpetrators for committing offense. Cybercrimes are borderless and sometimes transnational in nature means, it can occur anywhere there is access to the internet. This then makes international cooperation and investigative assistance particularly important.

Indian Penal Code 1860 (45 of 1860) - (commonly known as IPC):-

Sec. 3 – Punishment of Offences committed beyond, but which by law may be tried within, India. – Any person liable, by any Indian law to be tried for an offence committed beyond India shall be dealt with according to the provisions of this Code for any act committed beyond India in the same manner as if such act had been committed within India.

Sec.4 – Extension of Code to extra-territorial offences – The provisions of this Code apply also to any offence committed by-

(1) Any citizen of India in any place without and beyond India;

(2) Any person on any ship or aircraft registered in India wherever it may be.

Explanation – In this section the word “offence” includes every act committed outside India which, if committed in India, would be punishable under this Code.

The Code of Criminal Procedure 1898 (Act 5 of 1898) – (commonly known as Cr. P.C.) laid down the following provisions for trial of the offences committed outside India;

Sec 187. Power to issue summons or warrant for offences committed beyond local jurisdiction –
(1)- When a Magistrate of the first class sees reason to believe that any person within his local jurisdiction *has committed outside such jurisdiction (whether within or outside India*) an offence which cannot, under the provisions of sections 177 to 185 (both inclusive), or any other law for the time being in force, be inquired into or tried within such jurisdiction but is under some law for the time being in force triable in India, *such Magistrate may inquire into the offence as if it had been committed within such local jurisdiction* and compel such person in the manner herein before provided to appear before him, and send such person to the Magistrate having jurisdiction to inquire into or try such offence, or, if such offence is not punishable with death or imprisonment for life and such person is ready and willing to give bail to the satisfaction of the Magistrate acting under this section, take a bond with or without sureties for his appearance before the Magistrate having such jurisdiction.

(2)- When there are more Magistrates than one having such jurisdiction and the Magistrate acting under this section cannot satisfy himself as to the Magistrate to or before whom such person should be sent or bound to appear, the case shall be reported for the orders of the High Court.

Sec 166A – Letter of request to competent authority for investigation in a country or place outside India –

(1)-Notwithstanding anything contained in this Code, if, in the course of an investigation into an offence, an application is made by the investigating officer or any officer superior in rank to the investigating officer that evidence may be available in a country or place outside India, any Criminal Court may issue letter of request to a Court or an authority in that country or

place competent to deal with such request to examine orally any person supposed to be acquainted with the facts and circumstances of the case and to record his statement made in the course of such examination and also to require such person or any other person to produce any document or thing which may be in his possession pertaining to the case and to forward all the evidence so taken or collected or the authenticated copies thereof or the thing so collected to the court issuing such letter.

(2) The letter of request shall be transmitted in such manner as the Central Government may specify in this behalf.

(3) Every statement recorded or document or thing received under sub section (1) shall be deemed to be the evidence collected during the course of investigation under this Chapter

105 B. - Assistance in securing transfer of persons –

(1)- Where a Court in India, in relation to a criminal matter, desires that a warrant for arrest of any person to attend or produce a document or other thing issued by it shall be executed in any place in a contracting State, it shall send such warrant in duplicate in such form to such Court, Judge or Magistrate through such authority, as the Central Government may, by notification, specify in this behalf and that Court, Judge or Magistrate, as the case may be, shall cause the same to be executed.

(2)- Notwithstanding anything contained in this Code, if, in the course of an investigation or any inquiry into an offence, an application is made by the investigating officer or any officer superior in rank to the investigating officer that the attendance of a person who is in any place in a contracting State is required in connection with such investigation or inquiry and the Court is satisfied that such attendance is so required, it shall issue a summons or warrant, in duplicate, against the said person to such Court, Judge or Magistrate, in such form as the Central Government may, by notification, specify in this behalf, to cause the same to be served or executed.

(3)- Where a Court in India, in relation to a criminal matter, has received a warrant for arrest of any person requiring him to attend or attend and produce a document or other thing in that Court or before any other investigating agency, issued by a Court, Judge or Magistrate in a contracting State, the same shall be executed as if it is the warrant received by it from another Court in India for execution within its local limits.

(4)- Where a person transferred to a contracting State pursuant to sub- section (3) is a prisoner in India, the Court in India or the Central Government may impose such conditions as that Court or Government deems fit.

(5)- Where the person transferred to India pursuant to sub-section (1), or sub-section (2) is a prisoner in a contracting State, the Court in India shall ensure that the conditions subject

to which the prisoner is transferred to India are complied with and such prisoner shall be kept in such custody subject to such conditions as the Central Government may direct in writing.

Comprehensive Guidelines for Investigation Abroad & Issue of Letters Rogatory (Lr) Issued By MHA

COMPREHENSIVE GUIDELINES REFERRED TO IN LETTER NO. 25016/14/2007- LEGAL CELL DATED 31ST DEC., 2007 OF INTERNAL SECURITY DIVISION, MINISTRY OF HOME AFFAIRS REGARDING INVESTIGATION ABROAD AND ISSUE OF LETTERS ROGATORY AND ALSO THE PROCEDURE FOR EXTRADITION REQUESTS AND CONTACT WITH FOREIGN POLICE/LEGAL ATTACHÉS.

A. INVESTIGATION ABROAD

1. It may be necessary to gather information or conduct formal investigation abroad, in cases, where accused person(s) has escaped from the country after committing the crime or part of the crime has been committed outside the country or the witnesses and other material evidence are available in another country.

2. However, it may not be necessary to gather formal evidence in all such cases and in many cases/ enquiry; the investigation agency may only need information or lead in the first instance. The Investigation Agency may get informal information/material/leads collected through Interpol or diplomatic channels. [Intelligence sharing, however, is required to be done by designated intelligence agencies]. The International Police Cooperation Cell (hereinafter referred as IPCC) of CBI, New Delhi is the designated agency for routing requests for informal enquiries to be made with National Central Bureau of other countries, Interpol Headquarters as well as our Missions abroad.

3. For getting informal investigation conducted through the Interpol channels or our Missions abroad, a self-contained request, along with necessary details, may be addressed to Assistant Director, IPCC, Block # 4, CGO Complex, Central Bureau of Investigation, New Delhi. In case, information is to be collected/ enquiries are to be conducted in more than one country, separate self-contained requests may be sent for each country. The request may be routed through the head of Crime Investigation Department (CID) of the State Police.

4. The request must incorporate the following details:

   i. The FIR number along with names of the accused and sections of law under which case has been registered.

   ii. The gist of the allegations in the FIR/ Preliminary Enquiry or any other Investigation Process.

   iii. The detail of information required. In order to facilitate requested country/ its NCB providing information the specific relevant details must be furnished.

5. It is necessary that material furnished should be carefully examined and scrutinized at an appropriate level especially in regard to accuracy of facts and figures. It must be noted the information so collected cannot be treated as formal evidence.

B. VISIT OF POLICE OFFICERS ABROAD FOR INVESTIGATION

6. Sometimes, it may become necessary to send Police Officer(s) from India to foreign country for the purpose of execution of LR or for collecting information or leads during the course of

investigation of a case keeping in view the importance of the case and the complicated nature of offences under investigation.

7. As any police officer including that of the CBI would enjoy no Police powers in a foreign country and any such visit by a police officer without the express consent of any country may be considered interference in the sovereignty of that country unless some required formalities are observed.

8. When it is considered necessary to send a team of Officers abroad, the State Government will send a proposal to IPCC, CBI, India which in turn will obtain the approval of MHA for the proposed visit, whenever necessary.

9. The following information needs to be sent to the IPCC, CBI India for taking up the matter with the country to which such team is proposed to be sent:

   i. A brief note detailing the reasons for sending the team, nature of enquiries required to be made in the requested country. This is to enable the authorities to assess whether the request is justified.

   ii. All available particulars about identity or particulars of the person to be contacted or documents to be scrutinized etc. This would help the requested country to make all necessary preparations.

   iii. Information about penal offence to which mission relates.

   iv. Whether Article 3 of the ICPO (Interpol) Constitution or some other legal provision restricting international cooperation is attracted.

   v. Exact date and duration of the mission and information about the police officers such as their names and ranks.

   vi. Any other relevant information which may be relevant in processing such a request.

   The visit will not commence before the required permission is received. The officers must get in touch with Indian Mission on their arrival. In case, the country does not have a mission, the accredited mission for India may be kept informed as regards visit of the officers.

C. INVESTIGATION ABROAD UNDER SECTION 166-A CrPC, 1973

1. In order to conduct formal investigation and to collect evidence and gather material objects/documents Section 166-A of the Criminal Procedure Code 1973 lays down the procedure of sending 'Letter of Request' (Letters Rogatory) through a competent Court. Letters Rogatory is forwarded within the ambit of Mutual Legal Assistance Treaty (MLAT), Memorandum of Understanding (MoU)/ Arrangement etc. existing between India and requested country or on basis of reciprocity in case no such treaty and MoU exists. In certain cases, it may also be possible to use the provisions of an International Convention, providing for such mutual cooperation, to which both India and the requested country are signatory for sending such Letters Rogatory.

2. No request for issue of Letters Rogatory (Letter of Request) shall be brought before any Court by an Investigation Agency without prior concurrence of the Central Authority i.e. the Ministry of Home Affairs (MHA).

3. In case, it is considered necessary to get a Letters Rogatory (Letter of Request) issued, a self-contained proposal may be sent to Under Secretary (Legal), Internal Security Division, Ministry of Home Affairs, Lok Nayak Bhawan, New Delhi- 110 003 to be routed through the Home Department of the State in case of State Police, and directly to MHA in case of DSPE (CBI) for obtaining concurrence of the Government before filing an application in the Competent Court.

4. Before making a proposal to the MHA, the Investigating Agency concerned may examine the matter in detail whether it is absolutely necessary to get investigation conducted abroad for taking the case to a logical conclusion. The provisions of the MLAT, MoU, Arrangement or International Convention as well as requirement of the law of requested country such as principle of dual criminality, assurance of reciprocity etc., may be studied with view to determine that such a request would fall within the parameters of legal requirements of the requested country. It is important as it would have to be specifically mentioned as to under what provisions of Treaty, MoU, Arrangement or International Convention the request was being made. Where no such bilateral or multilateral arrangements exist Letters Rogatory may be made on the basis of assurance of reciprocity.

5. Certain countries do insist that a Letters Rogatory be sent in particular language or format. If so, the requirements thereof of making such a request may be studied to comply with them. Assistance of IPCC, CBI, New Delhi may be taken for the purpose, if required.

6. For obtaining the concurrence of MHA, the Investigating Agency concerned would send the following in triplicate:

i. A self-contained note containing brief facts of the case incorporating the allegations, names of the accused and particulars of the offences committed with details of Sections of Law and a copy of First Information Report (FIR). The FIR may be neatly word processed and must accompany with an English translation if written in vernacular.

ii. The need to conduct investigation abroad along with the legal opinion of Director of Prosecution or the senior most Law Officer commenting on the need for such Letters Rogatory (Letter of Request), that it would fall within the ambit of MLAT, MoU, Arrangement, International Convention and laws of the requested Country on the principles of dual criminality etc. Relevance of statement of witnesses to be examined and collection of documents/ material being requested to be seized to the investigation of the case may also be commented upon.

iii. The relevant provisions of the MLAT or MoU or Agreement or Arrangement or an International Convention under which the Letters Rogatory (Letter of Request) is to be made may be enclosed. In case it is to be sent on assurance of reciprocity the same may be mentioned.

iv. The draft application proposed to be filed in the competent court for issues of Letters Rogatory may be enclosed. The application should contain the following:

a. Background Note with brief facts of the case, the allegations and name of the accused and particulars of the offences committed with extract of Sections of Law and a neatly word processed copy of First Information Report (FIR) as enclosure .

b. The details of investigation to be carried in the requested country. Care must be taken that request made is specific as no country would allow phishing enquiries/ investigation.

c. Particulars of the witnesses to be examined, their identity and addresses if available along with detailed questionnaire for examination of each witness.

d. Description of the documents/articles to be collected and procedure for the same.

e. Extract of the corresponding Sections of laws of the requested country which would constitute an offence/s on similar allegations under investigation in India. It may be stated in particular if under the laws of the requested country principle of dual criminality or any other requirement is essential requirement for execution of Letters Rogatory.

f. Extract of relevant provisions of the MLAT, MoU, Arrangement or International Convention etc. providing for such assistance by the requested country.

g. Declaration that the proposed Letters Rogatory would be in compliance of all the requirements of the requested country and that the case under investigation is not of political, military, racial or religious character.

h. A draft Assurance of Reciprocity in case the request is being made to a country with whom no MLAT, MoU, Arrangement exists or the request does not fall within the ambit of an International Convention.

i. Whether a visit by Investigating or any other officer is proposed to assist the authorities in the requested country to execute the Letters Rogatory.

7. The following precautions may be taken by the Investigating Agency while preparing a Letters Rogatory:

i. The documents, photographs and objects, if enclosed with the Letters Rogatory, should be clearly marked and referred to in the body to enable the requested Authority to know clearly what is required to be done with them.

ii. All the photocopied papers/ documents enclosed must be legible and translated in the required language, if required.

iii. The Letters Rogatory should be neatly bound and page numbered.

iv. The authenticated translated copies, duly singed by a translator, be enclosed along with original LR, if required to be submitted in a language as prescribed in the MLAT, MoU, Arrangement or otherwise.

v. At least, five copies of the Letters Rogatory should be prepared including the original. Three copies along with the translated version, if any, would need to be sent to the MHA along with a copy to the International Police Cooperation Cell of CBI.

8. MHA may consult CBI whenever required and convey its concurrence to the proposal to be filed in the Competent Court for issue of a Letters Rogatory and also mark a copy of its concurrence to IPCC, CBI, New Delhi.

9. After obtaining the concurrence of the MHA, an application may be filed in the Court of competent jurisdiction for issue of Letters Rogatory addressed to the competent authorities of the requested country. The Competent Court may decide to issue a Letters Rogatory addressed to the competent authority in the requested country as prayed for or otherwise.

10. In case, the request is accepted, the Court would issue the Letters Rogatory under its seal and authority. A format and contents of the Letters Rogatory are given in the annexure to the guidelines.

D. PROCEDURE TO BE FOLLOWED AFTER ISSUE OF LR BY THE COMPETENT COURT

11. The Investigating agency will send three copies of the LR to IPCC, CBI, New Delhi and one copy to MHA. IPCC, CBI, New Delhi will forward the same to the competent authority in the requested country through the Indian Missions under intimation to MHA.

12. The Indian Mission will take prompt action to present/ send the LR to the competent authority and communicate the exact date of such presentation/ submission to IPCC, CBI, New Delhi. The Mission and IPCC will follow up the execution of LR with the competent authority in the requested country.

13. In event of requested country seeking clarifications, additional material etc., the Mission will directly communicate the same to the IPCC, CBI, New Delhi, who may take necessary action in the matter under intimation to MHA & MEA.

14. The execution report, along with evidence and supporting material, received from the requested country would be directly sent by our Mission abroad to the IPCC, CBI, New Delhi, who would in return send the same to the Agency concerned under intimation to MHA and MEA.

E. HANDLING OF INCOMING LETTERS ROGATORY (LR)

15. All incoming LR will be received by Under Secretary (Legal), Internal Security Division, Ministry of Home Affairs, Lok Nayak Bhawan, New Delhi – 110 003 and will be entrusted to an Investigation Agency (State Police/CBI) in consultation with Joint Director (Policy) in CBI.

16. Where LR needs to be executed through the State Police, it will be sent to IPCC, CBI for getting it executed by the State Police concerned.

17. The agency entrusted with the task of execution of LR will do so at the earliest. The letters rogatory would be executed in terms of the provisions of the MLAT, MoU, and Arrangement etc., if it exists with the requesting country otherwise the evidence shall be gathered under the provisions of Indian laws, as applicable.

18. The following precautions may be taken while preparing the Execution Report:

i. The documents, photographs and objects, if enclosed with the Execution Report, should be clearly marked and referred to in the body.

ii. All the photocopied papers/ documents enclosed must be legible and authenticated as per provisions of Indian Evidence Act unless otherwise provided in the MLAT, MoU, Arrangement etc.

iii. The Execution Report should be neatly bound and page numbered.

iv. At least, four copies of the Execution Report should be prepared including the original. Three copies including the original may be sent to the IPCC, CBI, New Delhi while a copy is retained by the executing agency for future reference.

19. After execution, the investigation agency will forward the execution report to the IPCC, CBI, New Delhi along with the evidence and material collected who will forward the same to the Central Authority of the requesting country through the MEA under intimation to MHA.

F. HANDLING OF EXTRADITION REQUESTS

20. Extradition if either done under Extradition Treaty or other Extradition Arrangement or Assurance of Reciprocity with the requesting country.

21. Extradition request can be normally made only after a charge-sheet has been filed in the court and the court has taken cognizance of the case. If the accused available in the other country is to be arrested and produced in the court in India, the requisite action to bring such accused to India is through Extradition Process and not through LR.

22. Extradition requests are not accepted for political offences. The principle of dual criminality is invariably followed for extradition requests. An accused extradited for a particular offence can be tried only for that offence by the receiving country.

i. The State investigating agency will send extradition requests to the IPCC, CBI, New Delhi through the State Home Department who would in turn send the same to MEA for further necessary action.

G. CONTACT BY AND WITH FOREIGN POLICE/ LEGAL OFFICERS/ATTACHÉS

23. Foreign Police Personnel/ Legal Attachés are not permitted to establish any direct contact with the police personnel at the State Level unless specifically authorized by MHA.

24. Any attempt by such foreign police /legal personnel to establish direct contact with the State Police Authorities should immediately be brought to the notice of MHA.

7.1. Format and the contents of the Letters Rogatory

The Competent Court after considering the request may decide to issue the Letters Rogatory (Letter of Request) as prayed for or otherwise. In case, the request is accepted the Court would issue the Letters Rogatory under its seal and authority. The Letters Rogatory, addressed to the Competent Authority of the requested country, would contain the declaration showing the competence and jurisdiction of the Court making to issue such request country. It would contain the following details and annexure:

1. Brief facts of the case, the allegations and name of the accused and particulars of the offences committed with extract of Sections of Law.
2. The details of investigation to be carried in the requested country.
3. Particulars of the witnesses to be examined, their identity and addresses, if available, along with detailed questionnaire for examination of each witness.
4. Description of the documents/articles to be collected and procedure for the same.
5. It may be mentioned that while conducting investigation in the requested State, the statements of witnesses may be recorded as per the requirement of law and procedure in vogue in the requested State and duly authenticated by the Officer recording the same. The documents may be requested to be collected in original and in case the authorities concerned are unable to part with original documents, duly authenticated true copies in the manner of certification provided in the law of the requested State be supplied. In case, the documents requested are “public documents” according to the law of requested State, then request may be made either to give original or to authenticate the documents

as provided under Section 78(6) of the Indian Evidence Act, 1872 i.e. a copy certified by the legal keeper thereof, with a certificate under the seal of Notary Public, or of an Indian Counsel or diplomatic agent, that the copy is duly certified by the officer having the legal custody of the original, and upon proof of the character of the document according to the laws of the requested country.

6. Request for permitting Officers of the Investigating Agency to present during execution of LR to render assist to the officers executing the request, if considered necessary.
7. A declaration that evidence made available would be used only in the case in which the request is made, if there is any such requirement.
8. It may be mentioned that as per Indian Law, it is not necessary to give any notice to the accused either before issuing the LR or before examining the same.

7.2. Annexure to be enclosed

I. A neatly word processed copy of First Information Report (FIR) as enclosure with English translation if recorded in vernacular.
II. Extract of the Sections of Law constituting the offences under investigation along with the Sections of Procedural Laws, if relevant.
III. Extract of the corresponding Sections of laws of the requested country which would constitute an offence/s on similar allegations under investigation in India. It may be stated in particular if under the laws of the requested country principle of dual criminality or any other requirement is essential requirement for execution of Letters Rogatory.
IV. Extract of relevant provisions of the MLAT, MoU, Arrangement or International Convention etc. providing for such assistance by the requested country.
V. Declaration that the case under investigation was not of political, military, racial or religious character, if required under the MLAT, MoU, Arrangement or International Convention under which the request was being made or otherwise.
VI. An Assurance of Reciprocity, duly issued by the authorized officer of the MHA under his seal and signatures, in case, the request is being made to a country with whom no MLAT, MoU, Arrangement exists or the request does not fall within the ambit of an International Convention.

Mutual Legal Assistance Treaties

As on date of writing this chapter, Agreement/ Treaty on Mutual Legal Assistance in Criminal matters is in operation with 39 countries, namely :

Sl. No.	Name of the Country	Year
1	Australia	2011
2	Azerbaijan	2013
3	Baharin	2005
4	Bangladesh	2011
5	Belarus	2006
6	Bosnia&Herzegovina	2010
7	Bulgaria	2008
8	Canada	1998
9	Ezypt	2009

10	France	2005
11	Hongkong	2009
12	Iran	2010
13	Indonesia	2011
14	Israel	2015
15	Kazakhstan	2000
16	Kyrgez Republic	2014
17	Kuwait	2007
18	Malaysia	2012
19	Maritius	2006
20	Mexico	2009
21	Mangolia	2004
22	Myanmar	2010
23	Russia	2000
24	Singapore	2005
25	South Africa	2005
26	South Korea	2005
27	Spain	2007
28	Sri Lanka	2010
29	Switzerland	1989
30	Sultanate of Oman	2015
31	Tajikistan	2003
32	Thailand	2004
33	Turkey	1993
34	Ukrain	2003
35	United Arab Emirates	2000
36	United Kingdom	1995
37	United States of America	2005
38	Uzbekistan	2001
39	Vietnam	2008

CHAPTER 8

Scene of Crime Management

CHAPTER 8

Scene of Crime Management

Why should you read this Chapter?

As our world changes and development in technology gets doubled up every year, there is always a possibility of crime happening online. Individuals and organisations are desperate to get help and protected against such heinous crimes. Law enforcement should be competent enough to face such dreadful wrong doings and the technology being used by them.

After reading this chapter, you would be able to:

- Identify various cybercrime the law enforcement are dealing with and their potential impact at individual or organizational level.
- Familiarize with principle of digital evidence

8. Introduction to crime management

Understanding and implementing good forensic practices is an essential part of being a good cybercrime investigator. It is important to understand both law and technology being a police officer. So as this book also focuses on the said two aspects. Cybercrime is always intertwined with cyber security and cyber forensics. In some cases, it is trans-border in nature, leading to technical & legal challenges. Many of them are discussed and mentioned in this book are drafted from real time use cases on how to manage crime evidence and crime efficiently at scene of crime.

8.1. Definitions Computer

Computers[12] are programmable electronic devices designed to accept data, perform prescribed mathematical and logical operations at high speed, and display the results of these operations.

According to IT ACT 2008, computer is defined as any electronic, magnetic, optical or other high-speed data processing device or system which performs logical, arithmetic, and memory functions by manipulations of electronic, magnetic or optical impulses, and includes all input, output, processing, storage, computer software, or communication facilities which are connected or related to the computer in a computer system or computer network.

Fig: Crime Scene

Source Code[13]: Every computer program is written in a programming language, such as Java, C/C++, or

[12] http://www.dictionary.com/browse/computer

[13] http://www.techterms.com/definition/sourcecode

Perl etc. These programs include anywhere between a few lines to millions of lines of text called source code.

According to IT ACT 2008, source code is defined as “Computer source code means the listing of programs, computer commands, design and layout, and program analysis of computer resource in any form.”

8.2. The principles of digital evidence

Principle 1: No action taken by law enforcement agencies, persons employed within those agencies or their agents should change data which may subsequently be relied upon in court.

Principle 2: In circumstances where a person finds it necessary to access original data, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions.

Principle 3: An audit trail or other record of all processes applied to digital evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result.

Principle 4: The person in charge of the investigation has overall responsibility for ensuring that the law and these principles are adhered to.

8.3. Steps to follow in the scene of crime

Step1: Before you twitch

- Consent search or search warrant
  - Understand the nature of the crime
  - Read the search warrant
- Concerns
  - Safety – It is a crime scene
  - Destruction of potential evidence
- Plan, Plan, Plan
  - The seizure
  - The collection techniques
  - The order of events

Step 2: What to take along

1. Evidence Tape
2. Chain of custody form
3. Inventory forms
4. Digital camera
5. Toolkit (Screw driver set with pentalobe Screwdriver for removing HDDs from Mac laptops)
6. Adhesive tape, Sticky note
7. New/ wiped pen drives, hard drives
8. Gloves, static wrist band
9. Write blockers (e.g. ATA, SATA, SCSI, firewire, USB, e-sata, SSD) with cables.
10. Hardware for Imaging (TD2U, Falcon, TrueImager) if available
11. Laptop with FTK (Crossover Tested)
12. Card readers
13. Magnifying glass, Flash Light

14. Faraday bag/Aluminium foil, Bubble wraps

Note: A write blocker is a device that allow acquisition of data on storage devices without compromising the integrity of the data. Different types of write blockers are available for acquiring data from hard disks, USB devices mentioned as e.g. above.

Step 3: Think about potential sources of digital evidence

1. RAM
2. HDD
3. Pen drives
4. Memory card
5. Mp3 player
6. CD/DVD/Blu-ray disk and other medias
7. Docs, notes, documentation etc.,

Step 4: Prior to serving the warrant

1. Start your investigation report
2. Understand the nature of the crime
3. Describe the role of computer or digital devise in the crime
4. Describe the limits of your investigation
5. Probable cause for seizure
6. What can be seized?
7. Where is the search to be conducted?

Fig: Sources of evidence

Step 5: seize what?

1. HDD
2. Removable media (pen drives, external hard disk)
3. RAM

Step 6: search or seizure where?

1. Secure the scene, restrict access
2. Preserve the area, no more finger prints
3. Ensure the safety of all concerned
4. Nobody touch nothing
5. Onsite, in the field office, In a lab
6. Disposal of seized items
7. Consider the size of seizure
8. Suspects
    a. Interview
    b. Passwords
    c. Location of data
    d. Installed software
    e. Network

Step 7: Tag & Bag

1. Photograph all components and connections
2. Pack it for transport and keep it away from EM

3. Collect all printed material
    a. Docs, Records, notes

Step 8: seizure

1. If the network is active
    a. Do not power down any networking gear
    b. They have no hard drives
    c. All evidence is volatile
    d. Acquire volatile evidence if required
    e. Seize the servers & workstations

2. Get the network admin to help
    They could corrupt the data or mislead the investigation so be careful

3. If off leave it off
    Tag & Bag
4. If ON
    a. Photographs and document especially communication ports
    b. An attempt may be made to access memory
    c. Disconnect the coms interface
    d. Tag & Bag

Step 9: security systems

1. Ingress/egress logs – timeline, ID's
2. Service provider
3. System information
4. Photograph & document location of all devises
5. Tag & bag all stored data & recorded data
6. Detailed documentation – you can't tag & bag

Step 10: Fax, Printer, Copiers, and ID printers

1. Dial list, e-mail address, times, logs, headers
2. Stored documents
    a. Sent
    b. To be sent
    c. Received – not opened
    d. Received – opened
    e. Photograph & personal information

Step 11: after pictures of an "on" PC

1. If the computer is an standalone PC
    a. Pull the plug
    b. Do not turn it off
2. If it is a laptop
    a. Pull the plug
    b. If it is still on it has a functioning battery
    c. Remove the battery
    d. Keep the battery separate

Step 12: Photos method

1. Items & placement

2. Each item
    a. Placement
    b. Model/serial numbers
    c. Front
    d. Back
    e. Cables
    f. Anything that might be of interest
    g. You only get one chance to record the original evidence
3. Floor plan
    a. Locate all equipment
    b. Number all equipment on the floor plan
    c. You will have to reconstruct
4. Photography or videography
    a. The entire area containing hardware & cables
    b. The screen of each computer that is ON

Step 13: Notes

1. Keep a very detailed log of every operation action
    a. Details
    b. Time
    c. Order
2. They can cover a lot of mistakes during the seizure & search
3. What did you do?
4. What reasons for doing it?
5. Itemize potential harm vs another way of doing it

8.4. Introduction to Hashing

8.4.1. Definition

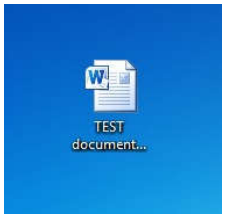
A hash value is a result of a calculation (hash algorithm) that can be performed on electronic file or entire hard drives contents. The result is also referred to as a checksum, hash code or hashes. The hash value is generated by a formula in such a way that it is extremely unlikely that some other file or entire hard drive will produce the same hash value.

8.4.2. Why Hashing?

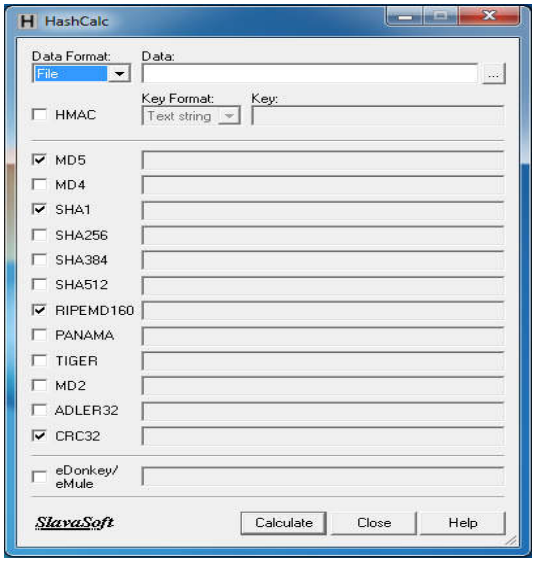
A **hash** value is used to ensure that the examined copy has not been altered i.e. the integrity of the digital evidence is ensured upon hashing. The hash value generated from a file becomes its “digital fingerprint”. MD5 and SHA are the two most common hash algorithms used in computer forensics.

8.4.3. Demonstration

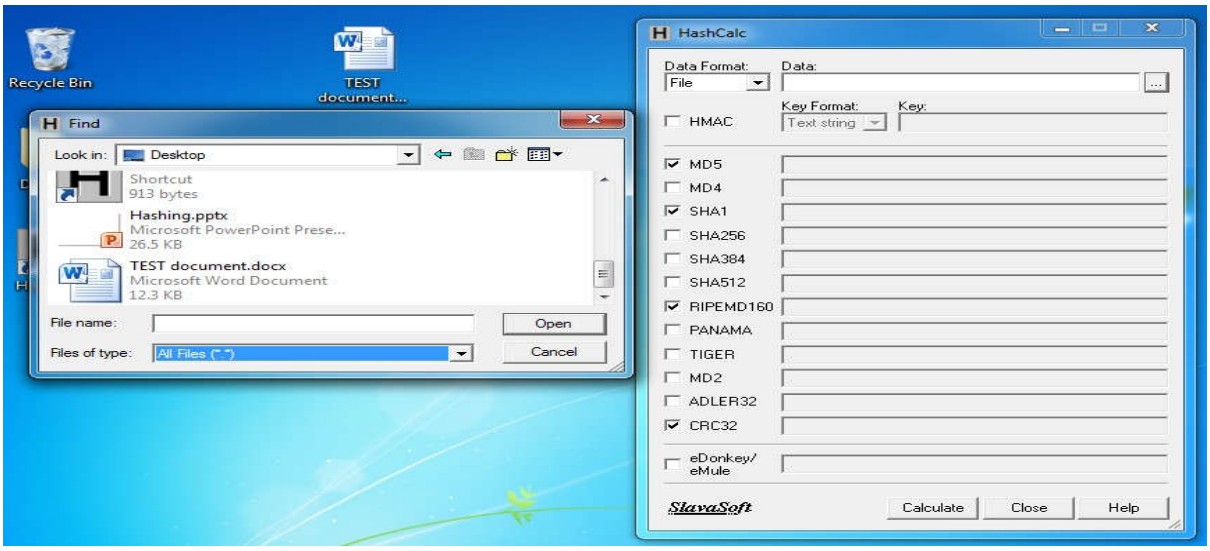
Step 1: choosing a file/image



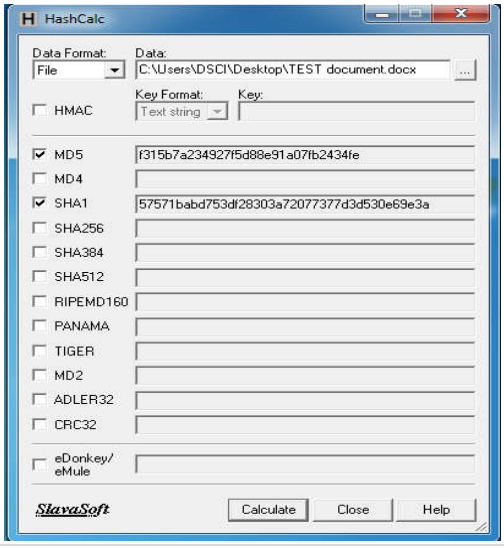
Step 2: In this demonstration Hashcalc software is used to calculate the hash of the file



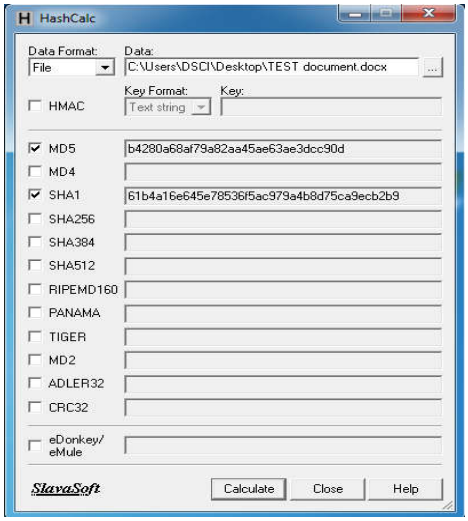
Step 3: Selecting a document to perform hashing



Step 4: press calculate button to generate hash value of a file.



Notice the change in the hash value when the original document is tampered



8.4.4. Indicative Free tools

- FTK Imager
- EnCase Forensic Imager
- Tableau Imager
- HashCalc
- Hashtab
- HashTool etc.

Note: Most of the Digital forensics tools have built in capability to calculate the hash value of digital evidence drive. It uses multiple algorithms like MD5, SHA to calculate the hash

CHAPTER 9

Cyber Laws

CHAPTER 9

Cyber Laws

Why should you read this Chapter?

As our world changes and development in technology gets doubled up every year, there is always a possibility of crime happening online. Individuals and organisations are desperate to get help and protected against such heinous crimes. Law enforcement should be competent enough to face such dreadful wrong doings and the technology being used by them.

After reading this book, you would be

- Identify various crimes with which law enforcement is dealing presently.
- Familiarize yourself with law related to cyber and legal aspects to curb them.

It is important to understand both law and technology being a police officer. So as this book also focuses on the said two aspects. Many of the sections you find in this manual are not comprehensively illustrated, to keep it more precise and reasonable. Mostly, it was only the gist of each element was selected and presented the same.

9.1. Introduction to Information Technology (IT) ACT:

- UN General Assembly enacted Model Law adopted by United Nations Commission on International Trade Law (UNICITRAL) by the resolution A/RES/51/162, dated 30 January 1997
- Then India passed the Information Technology ACT 2000 in May 2000 and came in to effectiveness on 17th October 2000
- This Information Technology Act is amended substantially through Information Technology Amendment Act 2008 which was passed by both the houses on 23 & 24 December 2008.
- This act got presidential assent on 5th Feb 2009 and came in to effectiveness on 27th October 2009.

9.2. Essence of information technology (IT) ACT

1. IT Act 2000 addressed the following issues
    a. Legal Recognition of Electronic Documents
    b. Legal Recognition of Digital Signatures
    c. Offenses and Contraventions
    d. Justice Dispensation Systems for Cybercrimes
2. ITAA, 2008 is often referred as the enhanced version of IT Act 2000 as it additionally focused on Information Security.
3. Several new sections on offences like Cyber Terrorism, Data Protection were added in ITAA, 2008.

9.3. Important sections under IT Act for discussion:

Section 43: Penalty and Compensation for damage to computer, computer system, etc.

If any person without permission of the owner or any other person who is in-charge of a computer, computer system or computer network –

(a) Accesses or secures access to such computer, computer system or computer network or computer resource

(b) downloads, copies or extracts any data, computer data base or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium;

(c) Introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network;

(d) damages or causes to be damaged any computer, computer system or computer network, data, computer data base or any other programmes residing in such computer, computer system or computer network;

(e) Disrupts or causes disruption of any computer, computer system or computer network;

(f) Denies or causes the denial of access to any person authorized to access any computer, computer system or computer network by any means;

(g) provides any assistance to any person to facilitate access to a computer, computer system or computer network in contravention of the provisions of this Act, rules or regulations made there under,

(h) Charges the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system, or computer network,

(i) Destroys, deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means (Inserted vide ITAA-2008)

(j) Steals, conceals, destroys or alters or causes any person to steal, conceal, destroy or alter any computer source code used for a computer resource with an intention to cause damage, he shall be liable to pay damages by way of compensation to the person so affected.

Section 66 Computer Related Offences

If any person, dishonestly, or fraudulently, does any act referred to in section 43, he shall be *punishable with imprisonment for a term which may extend to three years or with fine which may extend to five lakh rupees or with both.*

Section 66 B Punishment for dishonestly receiving stolen computer resource or communication device

Whoever dishonestly receives or retains any stolen computer resource or communication device knowing or having reason to believe the same to be stolen computer resource or communication device,

shall be *punished with imprisonment of either description for a term which may extend to three years or with fine which may extend to rupees one lakh or with both.*

Section 66C Punishment for identity theft

Whoever, fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other person, shall be *punished with imprisonment*

of either description for a term which may extend to three years and shall also be liable to fine which may extend to rupees one lakh.

Section 66D Punishment for cheating by personation by using computer resource

Whoever, by means of any communication device or computer resource cheats by personation, shall be *punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to one lakh rupees.*

Note: Section 66D is also called as 419 scam or advanced fee scam. The number "419" refers to the section of the Nigerian Criminal Code dealing with fraud. Most of the cheating by personation frauds like fake cheques, foreign money transfers, fake e-mailers, anonymous friend scams, phishing scams comes under this category.

Section 66E Punishment for violation of privacy

Whoever, intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person, shall be *punished with imprisonment which may extend to three years or with fine not exceeding two lakh rupees, or with both.*

Section 66F Punishment for cyber terrorism

(1) Whoever, - (A) with intent to threaten the unity, integrity, security or sovereignty of India or to strike terror in the people or any section of the people by –

(i) Denying or cause the denial of access to any person authorized to access computer resource; or

(ii) Attempting to penetrate or access a computer resource without authorisation or exceeding authorized access; or

(iii) introducing or causing to introduce any Computer Contaminant and by means of such conduct causes or is likely to cause death or injuries to persons or damage to or destruction of property or disrupts or knowing that it is likely to cause damage or disruption of supplies or services essential to the life of the community or adversely affect the critical information infrastructure specified under section 70, or

(B) knowingly or intentionally penetrates or accesses a computer resource without authorization or exceeding authorized access, and by means of such conduct obtains access to information, data or computer database that is restricted for reasons of the security of the State or foreign relations; or any restricted information, data or computer database, with reasons to believe that such information, data or computer database so obtained may be used to cause or likely to cause injury to the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence, or to the advantage of any foreign nation, group of individuals or otherwise, commits the offence of cyber terrorism.

(2) Whoever commits or conspires to commit cyber terrorism shall be punishable with imprisonment which may extend to imprisonment for life.

Section 67 provides for punishment to whoever transmits or publishes or causes to be published or transmitted, any material which is obscene in electronic form with imprisonment for a term which may extend to five years and with fine which may extend to Rs.1 lakh on first conviction. In the event of second or subsequent conviction the imprisonment would be for a term which may extend to ten years and fine which may extend to Rs. 2 lakhs. As per ITAA 2008, Section 67 is given as under:

Section 67 Punishment for publishing or transmitting obscene material in electronic form

Whoever publishes or transmits or causes to be published in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it, shall be *punished on first conviction with imprisonment of either description for a term which may extend to three years and with fine which may extend to five lakh rupees and in the event of a second or subsequent conviction with imprisonment of either description for a term which may extend to five years and also with fine which may extend to ten lakh rupees.*

Section 67 A Punishment for publishing or transmitting of material containing sexually explicit act, etc. in electronic form

Whoever publishes or transmits or causes to be published or transmitted in the electronic form any material which contains sexually explicit act or conduct shall be *punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees.*

Section 67 B Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc. in electronic form

Whoever,-

(a) Publishes or transmits or causes to be published or transmitted material in any electronic form which depicts children engaged in sexually explicit act or conduct or

(b) creates text or digital images, collects, seeks, browses, downloads, advertises, promotes, exchanges or distributes material in any electronic form depicting children in obscene or indecent or sexually explicit manner or

(c) Cultivates, entices or induces children to online relationship with one or more children for and on sexually explicit act or in a manner that may offend a reasonable adult on the computer resource or

(d) Facilitates abusing children online or

(e) records in any electronic form own abuse or that of others pertaining to sexually explicit act with children, *shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with a fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees*:

Provided that the provisions of section 67, section 67A and this section does not extend to any book, pamphlet, paper, writing, drawing, painting, representation or figure in electronic form

(i) The publication of which is proved to be justified as being for the public good on the ground that such book, pamphlet, paper writing, drawing, painting, representation or figure is in the interest of science, literature, art or learning or other objects of general concern; or

(ii) Which is kept or used for bonafide heritage or religious purposes

Section 67 C Preservation and Retention of information by intermediaries

(1) Intermediary shall preserve and retain such information as may be specified for such duration and in such manner and format as the Central Government may prescribe.

(2) Any intermediary who intentionally or knowingly contravenes the provisions of sub section (1) shall be punished with an imprisonment for a term which may extend to three years and shall also be liable to fine.

Section 69 Powers to issue directions for interception or monitoring or decryption of any information through any computer resource

Fig: phones

(1) Where the central Government or a State Government or any of its officer specially authorized by the Central Government or the State Government, as the case may be, in this behalf may, if is satisfied that it is necessary or expedient to do in the interest of the sovereignty or integrity of India, defense of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence relating to above or for investigation of any offence, it may, subject to the provisions of sub-section (2), for reasons to be recorded in writing, by order, direct any agency of the appropriate Government to intercept, monitor or decrypt or cause to be intercepted or monitored or decrypted any information transmitted received or stored through any computer resource.

(2) The Procedure and safeguards subject to which such interception or monitoring or decryption may be carried out, shall be such as may be prescribed.

(3) The subscriber or intermediary or any person in charge of the computer resource shall, when called upon by any agency which has been directed under sub section (1), extend all facilities and technical assistance to –

(a) Provide access to or secure access to the computer resource generating, transmitting, receiving or storing such information; or

(b) Intercept or monitor or decrypt the information, as the case may be; or

(c) Provide information stored in computer resource.

(4) The subscriber or intermediary or any person who fails to assist the agency referred to in sub-section (3) shall be punished with an imprisonment for a term which may extend to seven years and shall also be liable to fine.

Section 69 A Power to issue directions for blocking for public access of any information through any computer resource

(1) Where the Central Government or any of its officer specially authorized by it in this behalf is satisfied that it is necessary or expedient so to do in the interest of sovereignty and integrity of India, defense of India, security of the State, friendly relations with foreign states or public order or for preventing incitement to the commission of any cognizable offence relating to above, it may subject to the provisions of sub-sections (2) for reasons to be recorded in writing, by order direct any agency of the Government or intermediary to block access by the public or cause to be blocked for access by public any information generated, transmitted, received, stored or hosted in any computer resource.

(2) The procedure and safeguards subject to which such blocking for access by the public may be carried out shall be such as may be prescribed.

(3) The intermediary who fails to comply with the direction issued under sub-section (1) shall be punished with an imprisonment for a term which may extend to seven years and also be liable to fine.

Section 69B Power to authorize to monitor and collect traffic data or information through any computer resource for Cyber Security

Fig: indicative Servers

(1) The Central Government may, to enhance Cyber Security and for identification, analysis and prevention of any intrusion or spread of computer contaminant in the country, by notification in the official Gazette, authorize any agency of the Government to monitor and collect traffic data or information generated, transmitted, received or stored in any computer resource.

(2) The Intermediary or any person in-charge of the Computer resource shall when called upon by the agency which has been authorized under sub-section (1), provide technical assistance and extend all facilities to such agency to enable online access or to secure and provide online access to the computer resource generating, transmitting, receiving or storing such traffic data or information.

(3) The procedure and safeguards for monitoring and collecting traffic data or information, shall be such as may be prescribed.

(4) Any intermediary who intentionally or knowingly contravenes the provisions of subsection (2) shall be punished with an imprisonment for a term which may extend to three years and shall also be liable to fine.

Section 72 Breach of confidentiality and privacy

Save as otherwise provided in this Act or any other law for the time being in force, any person who, in pursuant of any of the powers conferred under this Act, rules or regulations made there under, has secured access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned discloses such electronic record, book, register, correspondence, information, document or other material to any other person shall be *punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.*

Section 72A Punishment for Disclosure of information in breach of lawful contract

Save as otherwise provided in this Act or any other law for the time being in force, any person including an intermediary who, while providing services under the terms of lawful contract, has secured access to any material containing personal information about another person, with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain discloses, without the consent of the person concerned, or in breach of a lawful contract, such material to any other person shall be *punished with imprisonment for a term which may extend to three years, or with a fine which may extend to five lakh rupees, or with both. Section 73 provides punishment for publishing a Digital Signature Certificate false in material particulars or otherwise making it available to any other person with imprisonment for a term which may extend to two years or with fine which may extend to Rs.1 lakh or with both.*

Section 76 Confiscation

Any computer, computer system, floppies, compact disks, tape drives or any other accessories related thereto, in respect of which any provision of this Act, rules, orders or regulations made there under has been or is being contravened, shall be liable to confiscation

Section 77 B Offences with three years imprisonment to be cognizable

Notwithstanding anything contained in Criminal Procedures Code, 1973, the offence punishable with imprisonment of three years and above shall be cognizable and the offence punishable with imprisonment of three years shall be bailable.

Section 78 Power to investigate offences

Notwithstanding anything contained in the Code of Criminal Procedure, 1973, a police officer not below the rank of Inspector shall investigate any offence under this Act.

Section 80 Power of Police Officer and Other Officers to Enter, Search, etc.

(1) Notwithstanding anything contained in the Code of Criminal Procedure, 1973, any police officer, not below the rank of an Inspector or any other officer of the Central Government or a State Government authorized by the Central Government in this behalf may enter any public place and search and arrest without warrant any person found therein who is reasonably suspected of having committed or of committing or of being about to commit any offence under this Act

Section 84 B Punishment for abetment of offences (Inserted Vide ITA-2008): Whoever abets any offence shall, if the act abetted is committed in consequence of the abetment, and no express provision is made by this Act for the punishment of such abetment, be punished with the punishment provided for the offence under this Act.

Section 84 C Punishment for attempt to commit offences

Whoever attempts to commit an offence punishable by this Act or causes such an offence to be committed, and in such an attempt does any act towards the commission of the offence, shall, where no express provision is made for the punishment of such attempt, be punished with imprisonment of any description provided for the offence, for a term which may extend to one-half of the longest term of imprisonment provided for that offence, or with such fine as is provided for the offence or with both.

9.4. Other important provisions under Cr.P.C. for performing search & seizure:

Section 165 Cr.P.C. Search by a police officer

(1) Whenever an officer in charge of police station or a police officer making an investigation has reasonable grounds for believing that anything necessary for the purposes of an investigation into any offence which he is authorised to investigate may be found in any place within the limits of the police station of which he is in charge, or to which he is attached, and that such thing cannot in his opinion be otherwise obtained without undue delay, such officer may, after recording in writing the grounds of his belief and specifying in such writing, so far as possible the thing for which search is to be made, search, or cause search to be made, for such thing in any place within the limits of such station.

(2) A police officer proceeding under sub-section (1), shall, if practicable, conduct the search in person.

(3) If he is unable to conduct the search in person, and there is no other person competent to make the search present at the time, he may, after recording in writing his reasons for so doing, require any officer subordinate to him to make the search, and he shall deliver to such subordinate officer an order in writing, specifying the place to be searched, and so far as possible, the thing for which search is to be made; and such subordinate officer may thereupon search for such thing in such place.

(4) The provisions of this Code as to search- warrants and the general provisions as to searches contained in section 100 shall, so far as may be, apply to a search made under this section.

(5) Copies of any record made under sub- section (1) or sub- section (3) shall forthwith be sent to the nearest Magistrate empowered to take cognizance of the offence, and the owner or occupier of the place searched shall, on application, be furnished, free of cost, with a copy of the same by the Magistrate.

Section 100 Persons in charge of closed place to allow search.
(1) Whenever any place liable to search or inspection under this Chapter is closed, any person residing in, or being in charge of, such place, shall, on demand of the officer or other person executing the warrant, and on production of the warrant, allow him free ingress thereto, and afford all reasonable facilities for a search therein.
(2) If ingress into such place cannot be so obtained, the officer or other person executing the warrant may proceed in the manner provided by sub- section (2) of section 47.

(3) Where any person in or about such place is reasonably suspected of concealing about his person any article for which search should be made, such person may be searched and if such person is a woman, the search shall be made by another woman with strict regard to decency.

(4) Before making a search under this Chapter, the officer or other person about to make it shall call upon two or more independent and respectable inhabitants of the locality in which the place to be searched is situate or of any other locality if no such inhabitant of the said locality is available or is willing to be a witness to the search, to attend and witness the search and may issue an order in writing to them or any of them so to do.

(5) The search shall be made in their presence, and a list of all things seized in the course of such search and of the places in which they are respectively found shall be prepared by such officer or other person and signed by such witnesses; but no person witnessing a search under this section shall be required to attend the Court as a witness of the search unless specially summoned by it.

(6) The occupant of the place searched, or some person in his behalf, shall, in every instance, be permitted to attend during the search and a copy of the list prepared under this section, signed by the said witnesses, shall be delivered to such occupant or person.

(7) When any person is searched under sub- section (3), a list of all things taken possession of shall be prepared, and a copy thereof shall be delivered to such person.

(8) Any person who, without reasonable cause, refuses or neglects to attend and witness a search under this section, when called upon to do so by an order in writing delivered or tendered to him, shall be deemed to have committed an offence under section 187 of the Indian Penal Code (45 of 1860).

9.5. Admissibility of electronic records under Indian Evidence ACT:

Section 65B of the Indian Evidence Act relates to admissibility of electronic records as evidence in the Court of law.

The computer holding the original evidence does not need to be produced in court.

65A. Special provisions as to evidence relating to electronic record

The contents of electronic records may be proved in accordance with the provisions of section 65B.

65B. Admissibility of electronic records

(1) Notwithstanding anything contained in this Act, any information contained in an electronic record which is printed on a paper, stored, recorded

Or

copied in optical or magnetic media produced by a computer (hereinafter referred to as the computer output) shall be deemed to be also a document, if the conditions mentioned in this section are satisfied in relation to the information and computer in question and shall be admissible in any proceedings, without further proof or production of the original, as evidence of any contents of the original or of any fact stated therein of which direct evidence would be admissible.

(2) The conditions referred to in sub-section (1) in respect of a computer output shall be the following, namely: -

(a) the computer output containing the information was produced by the computer during the period over which the computer was used regularly to store or process information for the purposes of any activities regularly carried on over that period by the person having lawful control over the use of the computer;

(b) during the said period, information of the kind contained in the electronic record or of the kind from which the information so contained is derived was regularly fed into the computer in the ordinary course of the said activities;

(c) throughout the material part of the said period, the computer was operating properly or, if not, then in respect of any period in which it was not operating properly or was out of operation during that part of the period, was not such as to affect the electronic record or the accuracy of its contents; and

(d) The information contained in the electronic record reproduces or is derived from such information fed into the computer in the ordinary course of the said activities.

(3) Where over any period, the function of storing or processing information for the purposes of any activities regularly carried on over that period as mentioned in clause (a) of sub-section (2) was regularly performed by computers, whether

(a) By a combination of computers operating over that period; or

(b) By different computers operating in succession over that period; or

(c) By different combinations of computers operating in succession over that period; or

(d) in any other manner involving the successive operation over that period, in whatever order, of one or more computers and one or more combinations of computers, all the computers used for that purpose during that period shall be treated for the purposes of this section as constituting a single computer; and references in this section to a computer shall be construed accordingly.

(4) In any proceedings where it is desired to give a statement in evidence by virtue of this section, a certificate doing any of the following things, that is to say, -

(a) Identifying the electronic record containing the statement and describing the manner in which it was produced;

(b) giving such particulars of any device involved in the production of that electronic record as may be appropriate for the purpose of showing that the electronic record was produced by a computer;

(c) dealing with any of the matters to which the conditions mentioned in sub-section (2) relate, and purporting to be signed by a person occupying a responsible official position in relation to the operation of the relevant device or the management of the relevant activities (whichever is appropriate) shall be evidence of any matter stated in the certificate; and for the purposes of this sub-section it shall be sufficient for a matter to be stated to the best of the knowledge and belief of the person stating it.

(5) For the purposes of this section, -

(a) Information shall be taken to be supplied to a computer if it is supplied thereto in any appropriate form and whether it is so supplied directly or (with or without human intervention) by means of any appropriate equipment;

(b) whether in the course of activities carried on by any official, information is supplied with a view to its being stored or processed for the purposes of those activities by a computer operated otherwise than in the course of those activities, that information, if duly supplied to that computer, shall be taken to be supplied to it in the course of those activities;

(c) A computer output shall be taken to have been produced by a computer whether it was produced by it directly or (with or without human intervention) by means of any appropriate equipment.

Refer template of 65B certificate in Annexure 1 and a sample certificate in Annexure 2

9.6. Few illustrations in which the certificates u/s 65B IEA may be obtained:

1. Photographs of Scene of Crime (SOC) is taken by ‘A’ using his digital camera. The memory card of the camera is primary evidence and should be seized. ‘A’ gives the IO the memory card. IO goes to a photo lab and asks ‘B’ to take hard copies of the photographs. Each photograph must be attested by ‘B’ who took the hard copy of the photograph and a certificate u/s 65B should be obtained from him.
2. ‘A’ takes Photograph/Video graph of scene of crime in his camera and copies it onto a CD and submits it to the IO. ‘A’ has to give section 65B of IEA certificate. If ‘A’ hand over the camera to ‘B’ and ‘B’ takes copy onto a CD, section 65B of IEA certificate should be obtained from ‘B’ and not from ‘A’.
3. ‘A’ murders ‘B’ in a shopping mall. The commission of crime was captured in the CCTV of the mall. Efforts should be taken to seize the original hard disk as it is primary evidence. If original hard disk/DVR is seized no section 65B of IEA is necessary as it is primary evidence. However if the video footage was copied on CD from the hard disk/DVR of the CCTV of the shopping mall, certificate u/s 65B of IEA has to be obtained from the person who copied the video footage onto the CD.
4. Incriminating evidence in the form of audio conversation related to a case was recorded by ‘A’ in his phone. He copied the audio clip in a memory card and produced it to the investigating officer. Efforts should be taken to get the original memory card. If not possible, the copy of the video clip stored in memory card should be authenticated by

a certificate u/s 65B of IEA from the person who copied the audio clip in the memory card.

5. 'A' threatens 'B' by sending emails. 'B' prefers a complaint along with the printouts of the threatening emails. Certificate u/s 65B of IEA has to be obtained from 'B'. 'B' has to attest each page of the printout of the threatening email.
6. 'A' sends abusive SMS to 'B'. 'B' prefers complaint along with a soft copy of SMS in CD & hard copy printouts. Certificate u/s 65B of IEA has to be obtained from 'B' for both the hard copy printout & the soft copy in CD. 'B' must attest each page of the hard copy of the printout.
7. 'A' posts obscene pictures in a WhatsApp group where 'B' is also a member. 'B' provides the soft copy of the chat details along with the alleged obscene images in both hard copy printouts and a soft copy in a CD/memory card along with the complaint. 'B' has to provide certificate u/s 65B of IEA for both the hard & soft copies. 'B' has to attest each page of the hardcopy printout.
8. 'A' creates a fake Facebook profile/account/page and posts obscene/derogatory materials about 'B'. 'B' prefers a complaint along with the screenshot printouts of the alleged Facebook profile/account/page. Certificate u/s 65B of IEA has to be obtained from 'B'. 'B' has to attest each page of the printout of the screen shot.
9. 'A' posts an anti-national/obscene video on YouTube. 'B' prefers a complaint in public interest along with the downloaded copy of the video in a pen drive/CD. Certificate u/s 65B of IEA has to be obtained from 'B' for the copy of the video in the pen drive/CD.
10. 'A' posts morphed pictures of 'B' in social media and portraying 'B' in an obscene or derogatory manner. 'B' prefers a complaint along with the screenshot printouts of the posts. Certificate u/s 65B of IEA has to be obtained from 'B'. 'B' has to attest each page of the printout of the screen shot.
11. A website was hacked/defaced. The access IP logs of the website were provided by 'Y', the system administrator. Certificate u/s 65B of IEA has to be obtained from 'Y'.
12. Investigation Officer obtains the IP logs of a suspect Facebook page. The soft copy of the IP logs provided by the Facebook was downloaded in a CD and hard copy printouts were also taken by him. I.O. has to issue certificate u/s 65 of IEA for authenticating both the CD and hard copy printouts.
13. The Time Zone Convertor was used by the I.O. to convert time given in UTC (Coordinated Universal Time) by email service provider or social network service provider into IST (Indian Standard Time). The screenshot printouts of the Time Conversion table have to be taken and the I.O shall issue certificate u/s 65B of IEA and attest the printouts.

9.7. Mapping of the offences against the relevant provisions of ITAA 2008

Sl. No.	Nature of complaint	Applicable section and punishment under ITAA 2008	Applicable section under other laws
1	Hacking of Email	Section 66 of ITAA 2008 - 3 years imprisonment or fine up to Rupees five lakh or both Section 66C of ITAA 2008 - 3 years imprisonment and fine up to Rupees one lakh	
2	Skimming of Credit Card/Debit Card	Section 66C of ITAA 2008- 3 years imprisonment and fine up to Rupees one lakh Section 66D ITAA 2008 - 3 years imprisonment and fine up to Rupees one lakh	Section 419 IPC - 3 years imprisonment or fine Section 420 IPC - 7 years imprisonment and fine

Sl. No.	Nature of complaint	Applicable section and punishment under ITAA 2008	Applicable section under other laws
3	Creating impersonating websites for cheating. e.g. Job frauds	**Section 66C of ITAA 2008** 3 years imprisonment and fine up to Rupees one lakh Section 66D ITAA 2008 3 years imprisonment and fine up to Rupees one lakh	**Section 419 IPC** 3 years imprisonment or fine Section 420 IPC 7 years imprisonment and fine
4	Receiving stolen data	**Section 66 B of ITAA 2008** 3 years imprisonment or Rupees one lakh fine or both	**Section 411 IPC** 3 years imprisonment or fine or both
5	Source code theft or modification of source code or data or information without authorization	**Section 66 of ITAA 2008** 3 years imprisonment or fine up to rupees five lakh or both	
6	Identity Theft (Election card, Aadhaar, DL etc.,)	**Section 66C of ITAA 2008** 3 years imprisonment and fine up to Rupees one lakh	
7	A Phishing e-mail is sent in the name of bank asking card number, expiry date, CVV number	**Section 66D of ITAA 2008** 3 years imprisonment and fine up to Rupees one lakh	**Section 419 IPC** 3 years imprisonment or fine or both
8	Capturing, publishing, or transmitting the image of the private area without any person's consent or knowledge	**Section 66E of ITAA 2008** Three years imprisonment or fine not exceeding Rupees two lakh or both	**Section 292 IPC** Two years imprisonment and fine Rupees 2000 and 5 years and rupees 5000 for second and subsequent conviction
9	Sending phishing mail to compromise government network with virus, APT's, worms etc.,	**Section 66 of ITAA 2008** 3 years imprisonment or fine up to Rupees five lakh or both **Section 66F of ITAA 2008** Life imprisonment	

Sl. No.	Nature of complaint	Applicable section and punishment under ITAA 2008	Applicable section under other laws
10	Perform DoS or DDoS attack on airlines, railways disrupting the essential servicers of the community	**Section 66 of ITAA 2008** 3 years imprisonment or fine up to Rupees five lakh or both **Section 66F of ITAA 2008** Life imprisonment	
11	Publishing or transmitting obscene material in electronic form	**Section 67 of ITAA 2008** first conviction - Three years and 5 lakh Second or subsequent conviction - 5 years and up to 10 lakh	**Section 292 IPC** Two years imprisonment and fine Rupees 2000 and five years and rupees 5000 for second and subsequent conviction
12	Publishing or transmitting of material containing sexually explicit act, etc., in electronic form	**Section 67A of ITAA 2008** first conviction - Five years and up to 10 lakh Second or subsequent conviction - 7 years and up to 10 lakh	Section 292 IPC - Two years imprisonment and fine Rupees 2000 and five years and rupees 5000 for second and subsequent conviction
13	Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc., in electronic form	**Section 67B of ITAA 2008** first conviction - Five years and up to 10 lakh Second or subsequent conviction - 7 years and up to 10 lakh	Section 292 IP - Two years imprisonment and fine Rupees 2000 and five years and rupees 5000 for second and subsequent conviction
14	Stealing data from armed forces, state/central government computers that have data or information related to national security.	**Section 66 of ITAA 2008** 3 years imprisonment or fine up to Rupees five lakh or both, **Section 66F of ITAA 2008** Life imprisonment	
15	Not allowing the authorities to decrypt all communication that passes through your computer or network.	**Section 69 of ITAA 2008** Imprisonment up to 7 years and fine	

Sl. No.	Nature of complaint	Applicable section and punishment under ITAA 2008	Applicable section under other laws
16	Intermediaries/ service providers (ISP, e-mail, Social media) not providing access to information stored on their computer to the relevant authorities	**Section 69 of ITAA 2008** Imprisonment up to 7 years and fine	
17	Posting defamatory messages on social media		**Section 500 IPC** 2 years or fine or both
18	E-mail Spoofing of a person and cheating	**Section 66C of ITAA 2008** 3 years imprisonment and fine up to Rupees one lakh	**Section 465 IPC** 2 years or fine or both **Section 468 IPC** 7 years imprisonment and fine

9.8. Cyber café guidelines

G.S.R. 315(E): In exercise of the powers conferred by clause (zg) of sub- section (2) of section 87 read with sub-section (2) of section 79 of the Information Technology Act, 2000 (21 of 2000), the Central Government hereby makes the following rules, namely:

9.8.1. Short title and commencement.

(1) These rules may be called the Information Technology (Guidelines for Cyber Cafe) Rules, 2011.

(2) They shall come into force on the date of their publication in the Official Gazette.

9.8.2. Definitions

(1) In these rules, unless the context otherwise requires,--

(a) "Act" means the Information Technology Act, 2000 (21 of 2000);

(b) "Appropriate Government" means the Central Government or the State Government or a Union Territory Administration;

(c) "Cyber Cafe" means cyber cafe as defined in clause (na) of sub-section (1) of section 2 of the Act;

(d) "Computer resource" means a computer resource as defined in clause (k) of sub- section (1) of section 2 of the Act;

(e) "Data" means data as defined in clause (o) of sub-section (1) of section 2 of the Act;

(f) "Information" means information as defined in clause (v) of sub-section (1) of section 2 of the Act; (g) "Intermediary" means an intermediary as defined in clause (w) of sub-section (1) of section 2 of the Act;

(h) "Registration Agency" means an agency designated by the Appropriate Government to register cyber cafe for their operation;

(i) "Log Register" - means a register maintained by the Cyber Cafe for access and use of computer resource;

(j) "User" means a person who avails or access the computer resource and includes other persons jointly participating in availing or accessing the computer resource in a cyber cafe.

(2) All other words and expressions used and not defined in these rules but defined in the Act shall have the meanings respectively assigned to them in the Act.

9.8.3. Agency for registration of cyber cafe.

(1) All cyber cafes shall be registered with a unique registration number with an agency called as registration agency as notified by the Appropriate Government in this regard. The broad terms of registration shall include:

I. name of establishment;
II. address with contact details including email address;
III. whether individual or partnership or sole properitership or society or company;
IV. date of incorporation;
V. name of owner/partner/properiter/director;
VI. whether registered or not (if yes, copy of registration with Registrar of Firms or Registrar of Companies or Societies); and
VII. Type of service to be provided from cyber cafe Registration of cyber cafe may be followed up with a physical visit by an officer from the registration agency.

(2) The details of registration of cyber cafe shall be published on the website of the registration agency.

(3) The Appropriate Government shall make an endeavour to set up on-line registration facility to enable cyber cafe to register on-line.

(4) The detailed process of registration to be mandatorily followed by each Registration Agency notified by the Appropriate Government shall be separately notified under these rules by the central Government.

9.8.4. Identification of User.

1) The Cyber Cafe shall not allow any user to use its computer resource without the identity of the user being established. The intending user may establish his identify by producing a document which shall identify the users to the satisfaction of the Cyber Cafe. Such document may include any of the following:
   I. Identity card issued by any School or College; or
   II. Photo Credit Card or debit card issued by a Bank or Post Office; or
   III. Passport; or
   IV. Voter Identity Card; or

V. Permanent Account Number (PAN) card issued by Income-Tax Authority; or
VI. Photo Identity Card issued by the employer or any Government Agency; or
VII. Driving License issued by the Appropriate Government; or
VIII. Unique Identification (UID) Number issued by the Unique Identification Authority of India (UIDAI).

(2) The Cyber Cafe shall keep a record of the user identification document by either storing a photocopy or a scanned copy of the document duly authenticated by the user and authorised representative of cyber cafe. Such record shall be securely maintained for a period of at least one year.

(3) In addition to the identity established by an user under sub-rule (1), he may be photographed by the Cyber Cafe using a web camera installed on one of the computers in the Cyber Cafe for establishing the identity of the user. Such web camera photographs, duly authenticated by the user and authorised representative of cyber cafe, shall be part of the log register which may be maintained in physical or electronic form.

(4) A minor without photo Identity card shall be accompanied by an adult with any of the documents as required under sub-rule (1).

(5) A person accompanying a user shall be allowed to enter cyber cafe after he has established his identity by producing a document listed in sub-rule (1) and record of same shall be kept in accordance with sub-rule (2).

(6) The Cyber cafe shall immediately report to the concerned police, if they have reasonable doubt or suspicion regarding any user.

9.8.5. Log Register.

(1) After the identity of the user and any person accompanied with him has been established as per sub-rule (1) of rule 4, the Cyber Cafe shall record and maintain the required information of each user as well as accompanying person, if any, in the log register for a minimum period of one year.

(2) The Cyber Cafe may maintain an online version of the log register. Such online version of log register shall be authenticated by using digital or electronic signature. The log register shall contain at least the following details of the user, namely

I. Name
II. Address
III. Gender
IV. Contact Number
V. Type and detail of identification document
VI. Date
VII. Computer terminal identification (viii) Log in Time
VIII. Log out Time

(3) Cyber Cafe shall prepare a monthly report of the log register showing date- wise details on the usage of the computer resource and submit a hard and soft copy of the same to the person or agency as directed by the registration agency by the 5th day of next month.

(4) The cyber cafe owner shall be responsible for storing and maintaining backups of following log records for each access or login by any user of its computer resource for at least one year:

I. History of websites accessed using computer resource al cyber cafe;
II. Logs of proxy server installed at cyber cafe. Cyber Cafe may refer to "Guidelines for auditing and logging - CISG-2008-01" prepared and updated from time to time by Indian Computer Emergency Response Team (CERT-In) for any assistance related to logs. This document is available at www.cert-in.org.in

(5) Cyber cafe shall ensure that log register is not altered and maintained in a secure manner for a period of at least one year.

9.8.6. Management of Physical Layout and computer resource

(1) Partitions of Cubicles built or installed if any, inside the Cyber Cafe, shall not exceed four and half feet in height from the floor level.

(2) The screen of all computers installed other than in Partitions or Cubicles shall face 'outward', i.e. they shall face the common open space of the Cyber Cafe.

(3) Any Cyber Cafe having cubicles or partitions shall not allow minors to use any computer resource in cubicles or partitions except when they are accompanied by their guardians or parents.

(4) All time clocks of the computer systems and servers installed in the Cyber Cafe shall be synchronised with the Indian Standard Time.

(5) All the computers in the cyber cafe may be equipped with the commercially available safety or filtering software so as to avoid as far as possible, access to the websites relating to pornography including child pornography or obscene information.

(6) Cyber Cafe shall take sufficient precautions to ensure that their computer resource are not utilised for any illegal activity.

(7) Cyber Cafe shall display a board, clearly visible to the users, prohibiting them from viewing pornographic sites as well as copying or downloading information which is prohibited under the law.

(8) Cyber Cafe shall incorporate reasonable preventive measures to disallow the user from tampering with the computer system settings.

(9) Cyber cafe shall maintain the user identity information and the log register in a secure manner.

(10) Cyber cafe shall also maintain a record of its staff for a period of one year

(11) Cyber cafe shall not misuse or alter the information in the log register.

9.8.7. Inspection of Cyber Cafe

(1) An officer authorized by the registration agency, is authorised to check or inspect cyber cafe and the computer resource of network established therein, at any time for the compliance of these rules. The cyber cafe owner shall provide every related

document, registers and any necessary information to the inspecting officer on demand.

CHAPTER 10

Case Studies

Chapter 10

10. Case Study 1: Job Fraud

Complaint: Mr. XXXXXXXXX, a manager of human resource of an MNC company located in Pune came to Cyber Crime Police Station and produced a written complaint along with some supporting documents on job fraud.

Brief facts: Some unknown people created an impersonating website of the company for running a fake recruitment drive with an intention of deceiving the job seekers. The fake website was redirected to the official website of the company. The job requirements were advertised through various online job portals and classifieds. The accused rented an office space in the same premises of the original company for doing fraudulent recruitment of the candidates. HRs were also hired to conduct the interview of shortlisted candidates. All the communication from the main accused is done through e-mail and phones to evade identification.

Laws Applied

► A case was registered in Cyber Crime Police Station Cr. No. xx/2017 U/S 66C & 66D of I.T. Act, 2000 and the investigation was taken up.

► IPC sections can be added accordingly.

Modus operandi:

► Accused impersonated the company website by creating a similar website using same fonts and there logo in www.zzz2.in similar to the original company website www.zzzz.in.org

► Accused had advertised about job openings in various online classifieds and communicated with many jobseekers offering guaranteed jobs in that MNC Company. The accused also informed all the candidates who contacted him for the job will be charging a nominal fee of INR 50000 for a job confirmation in that company. The candidates were asked to pay the money only after receiving the offer letter from the company.

► All the candidates were informed that a training will be organized for them 15 days before the interview is scheduled and it is free of charge. This was done to attract the candidates and gain their trust.

► The candidates completing the training were asked to appear for a written exam and personal interview in the yyy building, where the office of the complainant company presides. The victims were sent a fake offer letter mentioning the benefits to all the candidates who came for the interview.

10.1. Evidences provided by the complainant

During the course of investigation, the following documents were provided by the complainant for verification:

- An Email from the fraudulent containing job description and benefits
- Address of the interview location
- Fake website link
- Fake offer letter on the Company letter head
- Contact numbers
- SMS details

Investigation:

► Originating IP's were extracted after analyzing the e-mail headers sent to candidates from fraudsters.

► The details of CDR&CAF of the mobile numbers and physical address of IP's were obtained from respective service providers.

The authorities of yyy commercial building was contacted and following details were obtained:

- e-mail of person who booked the premises to conduct fake interview which is located in the same building of original company
- CCTV Clippings
- Mobile numbers
- Payment details for taking premises on rent

10.1.1. More details on investigation

► The registration and access details from the ESP (E-mail service provider) were also obtained.

► CDR & CAF of the mobile numbers were obtained from MSP (Mobile Service Providers).

► KYC details from the bank were obtained, during the investigation the beneficiary of the account revealed that they had sold their account to the accused. The access details obtained from the ESP was sent to ISP for the physical address which was traced to a cyber café!!

► A request is made to collect all the classifieds published by the accused to post the jobs e.g.: through Quikr, Olx etc. The registration details, ad posting IPs and ad details were obtained from classified sites like Quikr and OLX were obtained. The email address used in registration was sent to ESP's to get the registration and access details.

► The service provider of IP's received from ESPs were identified and requisition was sent to collect the physical address. Again physical address which was traced to the same cyber café!!

► The registrant details were obtained using who is domain lookup of **www.zzz2.in**. The warrant was obtained to search the cyber cafe, the owner of the cyber café was questioned. A team went to cyber café & the owner was asked to produce cyber café logs and CCTV clippings if any. There was no information in log book which just had name, in time, out time, sign and no CCTV was installed.

► After asking multiple questions, the owner of cyber café recognized that one of his regular customer by name **a-1** who used to do recruitment activities of various companies including the complainants company through accused own laptop. He then produced his laptop.

► Instructions were given to the owner of cyber café to inform the police when the suspect visits the café. The information was received from the owner of cyber café about the presence of accused in his café.

► The accused was arrested & was directed to take the team to his home for seizing laptop, mobile phone, Pen Drives etc.,

► The mobile number was identified through an **USSD** (**Unstructured Supplementary Service Data**) **Code.** The mobile number was matching with the number used to contact the victims. It was registered with a fake address.

► The laptop was seized and later was analyzed using a write blocker to create the image. Using sophisticated forensic tools like enCase, IEF and Belkasoft evidence finder relevant artifacts were extracted from the disk image. The documents containing company letter heads, E-mail sent to victims were identified.

- ► IMEI's of seized mobile handsets were matched with the IMEI's of some suspected number CDR's. Three more accused were identified and arrested and all of them confessed about the crime that they had committed
- ► Twenty candidates deposited money in the fake bank account where all the accused used to share the money deposited. The case came to light when one of the candidate visited the original company with a fake offer letter.

10.2. Case study 2: Sharing of morphed obscene contents through e-mail & Facebook

Complaint: Mrs. XXXXXXXXX, a senior software engineer of an MNC company came to Cyber Crime Police Station and produced a written complaint along with e-mail containing links of her obscene morphed image circulated on Facebook.

Brief facts: A suspect started sending mails from XYZ@yahoo.com to complainant's mail id Aisxxxxa@yyy.com to defame the complainant, published her morphed photograph in an obscene manner the Facebook account (http:/www.facebook.com/DesiSexyAunties), with a criminal intimidation, and also he communicated through mail that he will upload the pictures in multiple websites if the complainant doesn't respond to him.

Laws Applied

- ► A case was registered in Cyber Crime Police Station Cr. No. xx/2016 U/S 67 of I.T. Act, 2000 and the investigation was taken up.
- ► IPC sections can be added accordingly.

Investigation:

- ► The printouts of e-mails along with the full header details are taken with the help of complainant by logging in to her e-mail account.
- ► A notice under 79(2)(c) & (3)(b) of the Information Technology Act, 2000 read with The Information Technology (Intermediaries Guidelines) Rules, 2011 is sent to the yahoo for obtaining registration and access details of the suspects account.
- ► A notice under 79(2)(c) & (3)(b) of the Information Technology Act, 2000 read with The Information Technology (Intermediaries Guidelines) Rules, 2011 is sent to Facebook for taking down the content and requesting access details of the post.
- ► Yahoo Inc, didn't provide any information citing the reason that e-mail ID belongs to US domain and bound by USA laws.
- ► Facebook Inc, didn't provide any information as well and mentioned that the desired information by the IO will be provided through MLAT.
- ► The IO analysed the header and identified the originating IP. The service provider details of the IP was found by searching the WHOIS database.
- ► The IP range was belonging to the Airtel.
- ► The date and time in the e-mail header was noted. The time zone is converted from SGT to IST before requesting the IP details from the service provider.
- ► A notice under 91 CrPC is issued to obtain the physical address from the service provider.
- ► It was traced to a PG. A team went there for further investigation. The connection was in the name Mr. XXX. After questioning, he informed that he was not using Wi-Fi on the said date as he went to his native place to visit his parents. He informed his roommate Mr. YYY is also using the same Wi-Fi and the bill is split between them.
- ► Mr. YYY was questioned. His laptop was seized. The image was searched in the laptop. It was not found (stored) in the laptop. The laptop was further analysed

using EnCase, Belkasoft evidence centre and the obscene image of the complainant was recovered.

- The accused was instructed to open the e-mail id (XYZ@yahoo.com), which was used to send morphed photo of complainant to complainant's mail id Aisxxxxa@yyy.com. The screen shots of the mails sent to the victim were taken and incorporated in the Mahazar.
- The seized laptop is sent to CFSL for providing expert opinion.

.

10.3. Case study 3: E-mail spoofing case

Complaint: Mrs. XXXX, a CFO of an import & export corporation came to Cybercrime Police Station and produced a written complaint along with e-mail received from her CEO for transferring Rs. 50 Lakhs to two different bank accounts.

Brief facts: A suspect sent a mail to Mrs. XXXX, CFO of the corporation spoofing the e-mail ID xyz@ycorp.in of the CEO of the corporation. The accused then directed to transfer sum of Rs 50 Lakhs to two different bank accounts to close an import deal. The CEO was out of the country for concluding a business deal. Mrs. XXXX immediately transferred the said amount to two different bank account details mentioned in the e-mail. When the CEO came back to India, he held a meeting with CFO & other board members. The CFO informed about the money she transferred. He informed her that he never made such request. Mrs. XXXX lodged a complaint in the cybercrime police station.

Laws Applied

- A case was registered in Cyber Crime Police Station Cr. No. xx/2017 U/S 66C & 66D of I.T. Act, 2000 and the investigation was taken up.
- IPC sections can be added accordingly.

Investigation:

- The printouts of e-mails along with the full header details are taken with the help of complainant by logging in to her e-mail account.
- The header was analyzed, the originating IP was outside the India.
- The two bank accounts were frozen by the IO and KYC details was obtained by issuing a notice under 91 CrPC
- The address provided to the bank was verified and found out to be fake.
- The CDR and CAF of the phone numbers given to the banks were analysed. The address in the CAF and number used to contact victims was fake.
- In one of the bank, it was mandatory for a person to introduce for opening an account. Mr zzz had introduced the accused to the bank.
- Mr. zzz was traced and he gave the information that account holder is a Nigerian national.
- He had recently withdrawn the money from the same branch through cheque as per the statement from his account. The CCTV clip was requested from the bank by issuing notice under 91 CrPC
- Mr. zzz identified the accused. Accused came back to the same bank to withdraw the amount in the account. The bank alerted the authorities and he was arrested.

10.4. Case study 4: Matrimonial Fraud

Complaint: Ms. XXXX, a project manager from an MNC came to the Cybercrime Police Station and produced a written complaint that she was duped of Rs. 20 Lakhs by the accused on the matrimonial website.

Brief facts: Ms. XXXX, was registered in a matrimonial website www.xxxmatrimony.com. She was approached by a person with the profile mentioning as Director of a reputed MNC company in England. She liked the profile and they exchanged the numbers. They started communication on the phone, WhatsApp, Facebook. They both exchanged their pictures talked about future plans and many other things. Ms. XXXX thought she found a great match in the matrimonial site. After few months of communication he told his funds are tied up in the stocks and he told that he wanted to buy a flat in her name. He shared the property details and requested her to transfer a down payment of Rs. 500000 to a bank account number.

Laws Applied

- A case was registered in Cyber Crime Police Station Cr. No. xx/2017 U/S 66C & 66D of I.T. Act, 2000 and the investigation was taken up.
- IPC sections can be added accordingly.

Investigation:

- The creation and access logs were requested from the matrimonial website and Facebook by issuing a notice under 79(2)(c) & (3)(b) of the Information Technology Act, 2000 read with The Information Technology (Intermediaries Guidelines) Rules, 2011
- The numbers used by the suspect was now inactive
- The logs received by both matrimonial website and Facebook
- All the IP addresses were analyzed and it was traced outside India
- The websites were accessed by accused through proxy IP addresses by installing a proxy software on the system.
- One IP in the Facebook access logs was of Indian service provider. The physical address of the IP address was requested from the service provider. It was traced to a cyber café
- The owner of the cyber café was not maintaining logs of the people using the facility. Upon questioning the owner based on the date and analyzing the PC's in the cyber café. One system was installed with a proxy software. The suspect was zeroed in based on the information given by the owner of the cyber café. Since the suspect was using the same system whenever he visited the cyber café.
- The suspect's address was known to one of the customer and he took the team to suspect's residence. The suspect was arrested and produced before the court.

The below cases are convicted in the court.

10.5. Case study 5: Posting obscene content in yahoo group (State of Tamil Nadu Vs Suhas Katti)

Brief facts:

This case led to the first conviction under the Information Technology Act, 2000. The victim was being harassed by the accused, Suhas Katti, when she refused to marry him.

- The accused posted of obscene, defamatory and annoying message about a divorcee woman in the yahoo message group.
- E-Mails were also forwarded to the victim for information by the accused through an impersonating e-mail account opened by him in the name of the victim.
- The posting of the message resulted in annoying phone calls to the victim in the belief that she was soliciting.
- The Police traced the accused to Mumbai and arrested. The accused was a known family friend of the victim and was reportedly interested in marrying her.
- The victim however married another person later ended in divorce. The accused started contacting her once again. On her reluctance to marry him, the accused took up the harassment through the Internet.
- The Defence argued that the offending mails would have been sent either by her ex-husband or the complainant herself to implicate the accused as accused alleged to have turned down the request of the complainant to marry her.
- Further the Defence counsel argued that some of the documentary evidence was not sustainable under Section 65 B of the Indian Evidence Act. However, the court based on the expert witness and other evidence produced including the witness of the Cyber Cafe owners came to the conclusion that the crime was conclusively proved.

Laws Applied

- Charge Sheet was filed u/s 67 of IT Act 2000, 469 and 509 IPC before The Hon'ble Addl. CMM Egmore

Judgment

- Ld. Additional Chief Metropolitan Magistrate, Egmore, delivered the judgement on 5-11-04 as follows: "The accused is found guilty of offences under section 469, 509 IPC and 67 of IT Act 2000 and the accused is convicted and is sentenced for the offence to undergo rigorous imprisonment for 2 years under 469 IPC and to pay fine of Rs.500/- and for the offence u/s 509 IPC sentenced to undergo 1 year simple imprisonment and to pay fine of Rs.500/- and for the offence u/s 67 of IT Act 2000 to undergo rigorous imprisonment for 2 years and to pay fine of Rs.4000/- All sentences to run concurrently. The accused paid fine amount and he was lodged at Central Prison, Chennai.

10.6. Case study 6: Harassing a lady by posting obscene comments (State Vs Jayanta Das (Odisha)

Brief facts:

The case led the first ever conviction in a cyberporn case in the state of Odisha, a court in Puri on Friday sentenced an RTI activist to six years in prison and imposed a fine of Rs 9,000.RTI activist Jayant Kumar Das was arrested by the state Crime Branch in 2012 for allegedly making obscene comments about a journalist's wife on a porn site.

- Complainant lodged the written report Baseli Sahi Police Station, Puri alleging therein that on dtd. 18.03.12 while he was in his home at about 12.42 A.M. he got a telephone message from one mobile phone calling him as “Hello Suchitrarani” “Got your listing on desi hunt”.
- He immediately verified the web site where he found a profile opened in his wife's name Suchitrarani vide member I.D:-018072 in Desi Hunt.com. He also found another profile was opened in the same website vide No. 15932 as “ Suchitrarani wife swapping in India, desi couples, Indian”, wherein his two cell phones were given for contact.
- Prior to three months back from that date i.e. on 18.03.12 every day the complainant used to get numbers of telephonic calls and message out of state, that a profile has been opened in his wife's name in “ Wife sharing Group” (WSG) and his mobile phone numbers have been attached there. Due to social stigma, prestige he did not disclose the matter to anyone.
- The complainant being a journalist by profession the informant had published number of news items against the accused Jayant Kumar Das, Managing Partner of one AKJK Enterprisers of Nabakaleba, Puri Town who was lending loans to private persons and has allegedly cheated the borrowers.
- The accused created profile in retaliation for writing and publishing an article against him in THE PRAJATANTRA newspaper by the complainant.

Laws Applied

- Charge Sheet was filed U/s.292/465/469/500 I.P.C. r.w. Section 66(C)/67/67(A) of the Information Technology Act,2008

Judgment

The accused sentenced to to undergo R.I. for a term of *six months* and is liable to pay the fine of Rs. 500/- in default S.I. for 15 days for the commission of offence U/s. 292 I.P.C. Further he is sentenced to undergo R.I. for a term of *six months* and is liable to pay the fine of Rs. 500/- in default S.I. for 15 days for the commission of offence U/s. 465 I.P.C. Further he is sentenced to undergo R.I. for a term of *one year* and is liable to pay the fine of Rs. 1,000/- in default S.I. for one month for the commission of offence U/s. 469 I.P.C. Further he is sentenced to undergo S.I. for a term of *six months* and is liable to pay the fine of Rs. 500/- in default S.I. for 7 days for the commission of offence U/s. 500 I.P.C. Further he is sentenced to undergo R.I. for a term of *one year* and is liable to pay the fine of Rs. 1,000/- in default S.I. for one month for the commission of offence U/s. 66(C) of I.T. Act, 2008. Further he is sentenced to undergo R.I. for a term of *six month* and is liable to pay the fine of Rs. 500/- in default S.I. for 15 days for the commission of offence U/s. 67 of I.T. Act, 2008. Further he is sentenced to undergo R.I. for a term of *two years* and is liable to pay a fine of Rs. 5000/- in default S.I. for two months for the commission of offence U/s. 67(A) of I.T. Act, 2008. However, all the substantive sentences of imprisonment shall run consecutively.

LAB EXERCISES

Lab Exercises

Exercise 1: Recover deleted files from pen drive

What you will need?

I. A USB drive that should contain files in multiple formats like *.pdf, *.txt, *.jpeg, *.doc, *.ppt, *.xls, *.3gp, *.mp3 etc.
II. A data recovery software like Recuva, Pandora recovery, undelete 360,

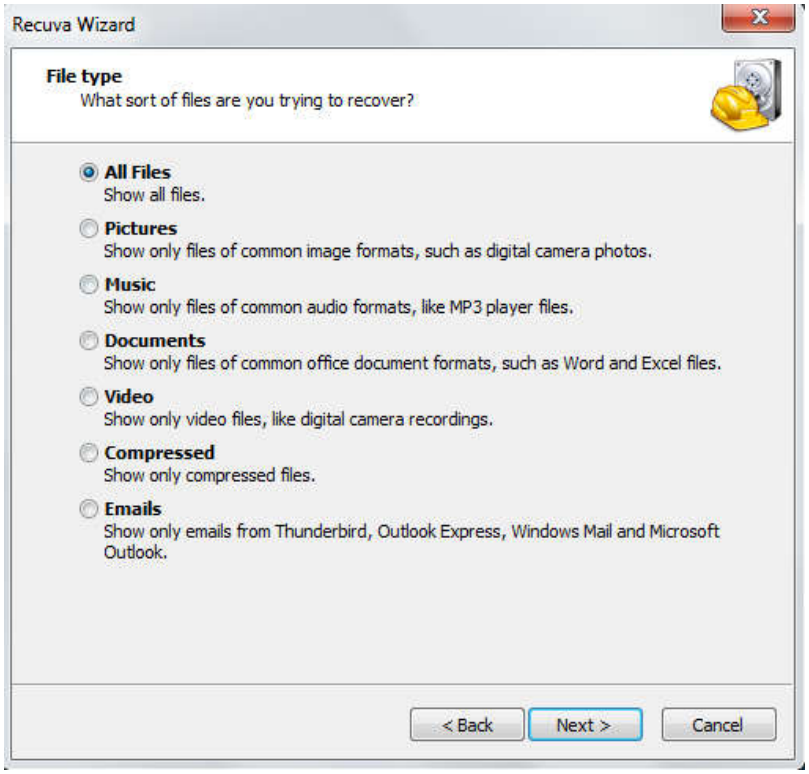
Steps involved in the exercise

1. Install Free/open source data recovery software's on the desktop
2. Insert USB drive containing files in multiple formats mentioned above
3. Delete 1 image file (*.txt) 1 audio file (*.mp3)
4. Try recovering the same using data recovery software.

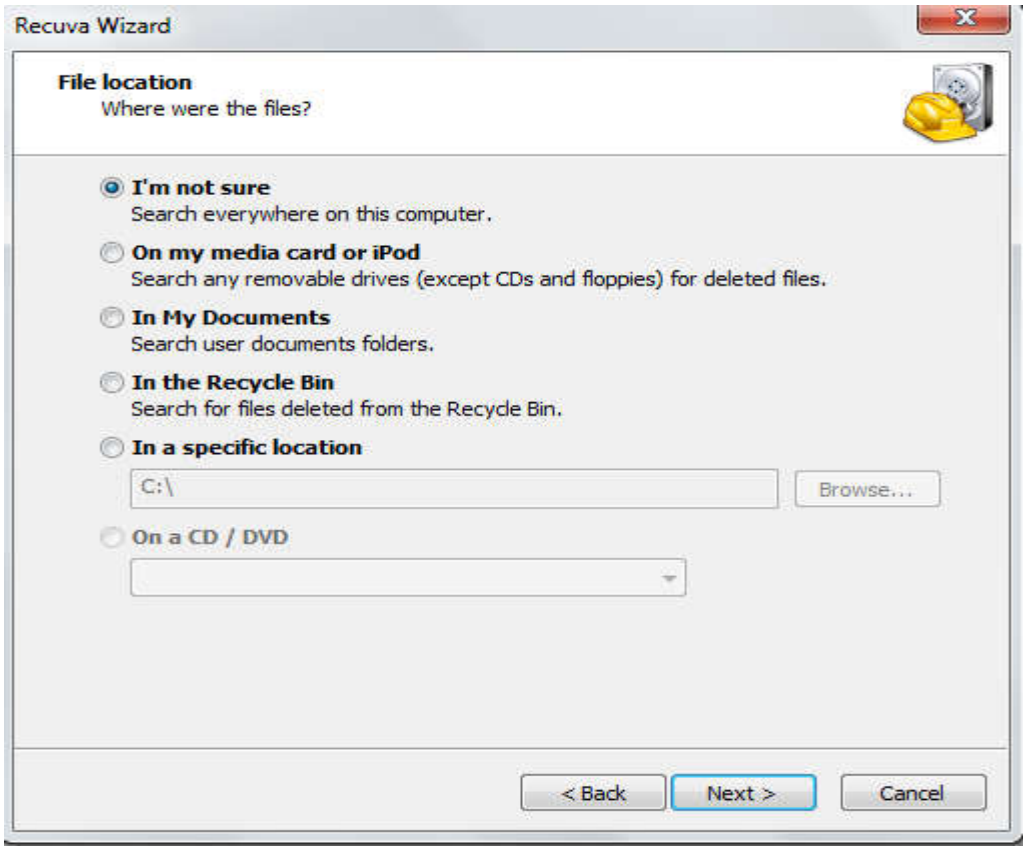
Demonstration: In this demonstration we are using Recuva to recover data

Step 1: Click on the Icon to open Recuva

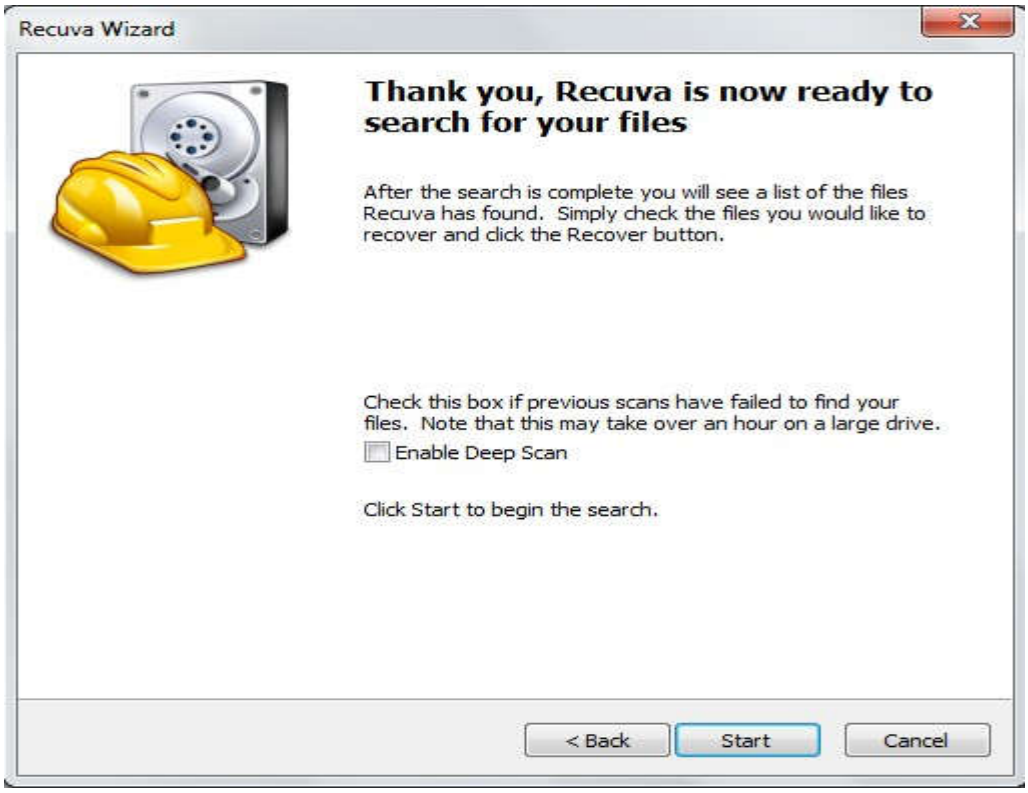
Step 2: Select the file type you want to recover. In this case all files are selected



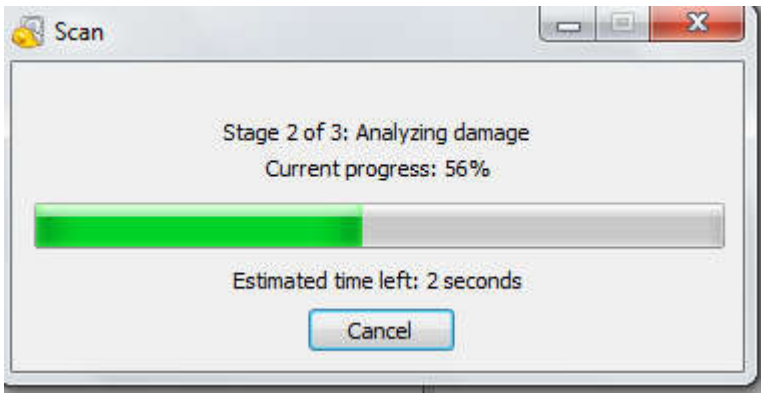
Step 3: Select the location where you want to recover the file. If you are not sure select the first option as illustrated below.



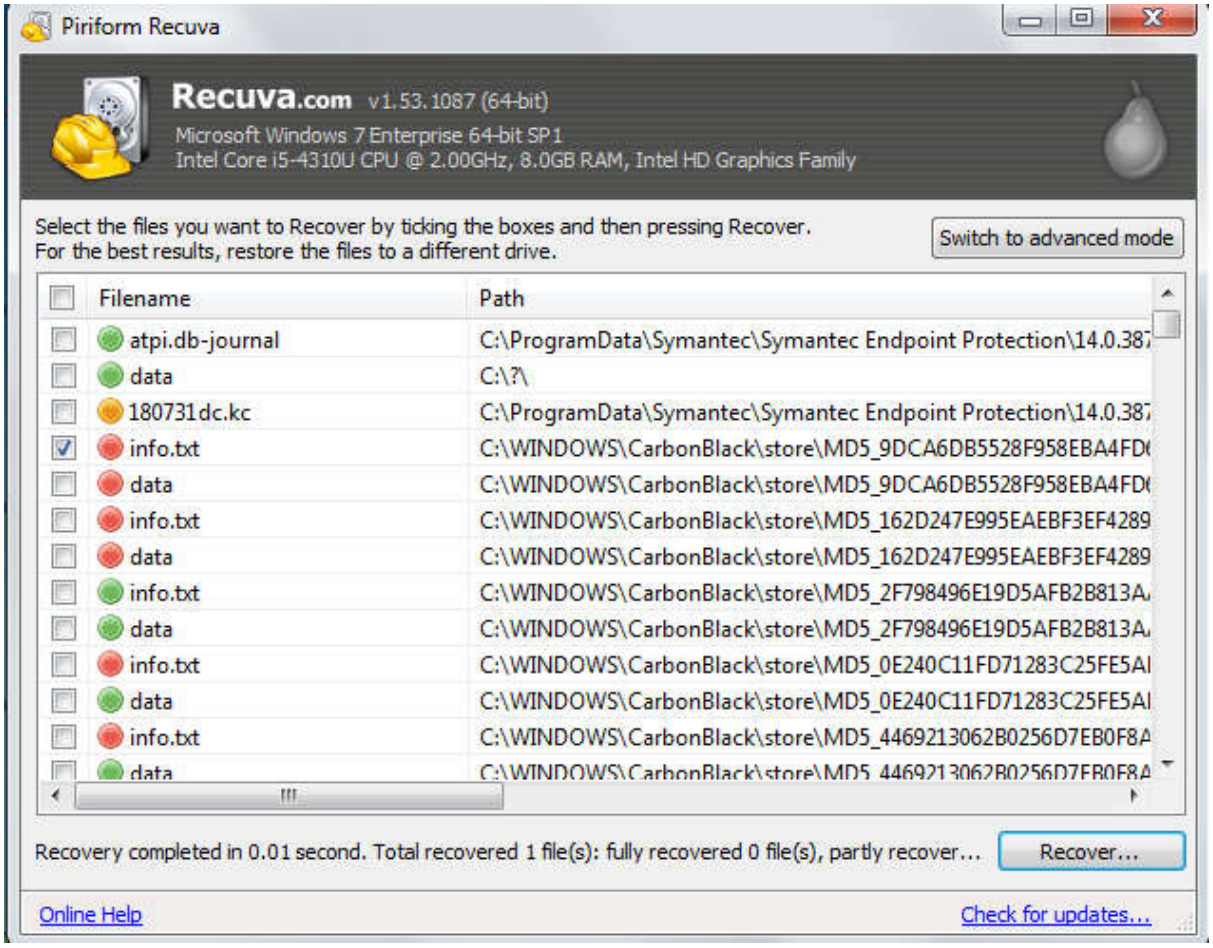
Step 4: Start scan, if the files can't recovered in this mode, open the software and select deep scan



Step 5: The software is showing the progress of the recovery



Step 6: select files to be recovered. In this example, info.txt is selected for recovery



Step 7: Deleted text file recovered from the software

Exercise 2: Imaging the RAM

What you will need?

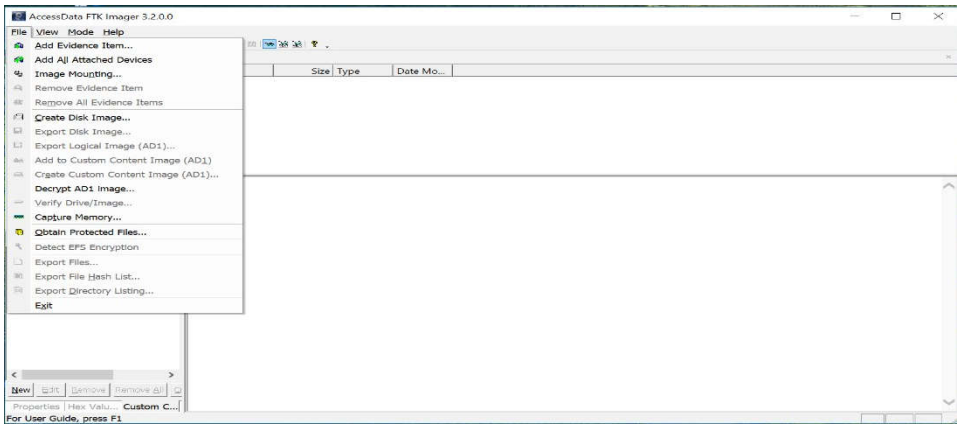
I. A empty pen drive
II. A free/open source RAM acquisition software or software having capability of imaging RAM e.g. FTK Imager, Belkasoft Live RAM Capturer, Magnet RAM Capture, DumpIt

Steps involved in the exercise

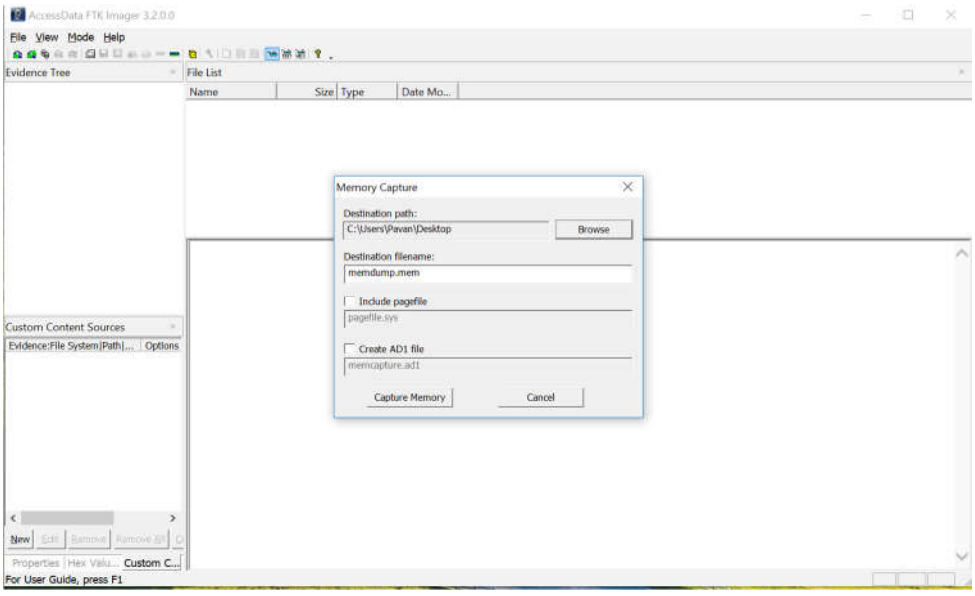
1. Install free/open source forensic imaging software
2. Insert a pen drive in the USB port of the desktop
3. Acquire the RAM in installed in the desktop by giving the destination to the pen drive

Demonstration: In this demonstration we are using FTK imager for capturing RAM

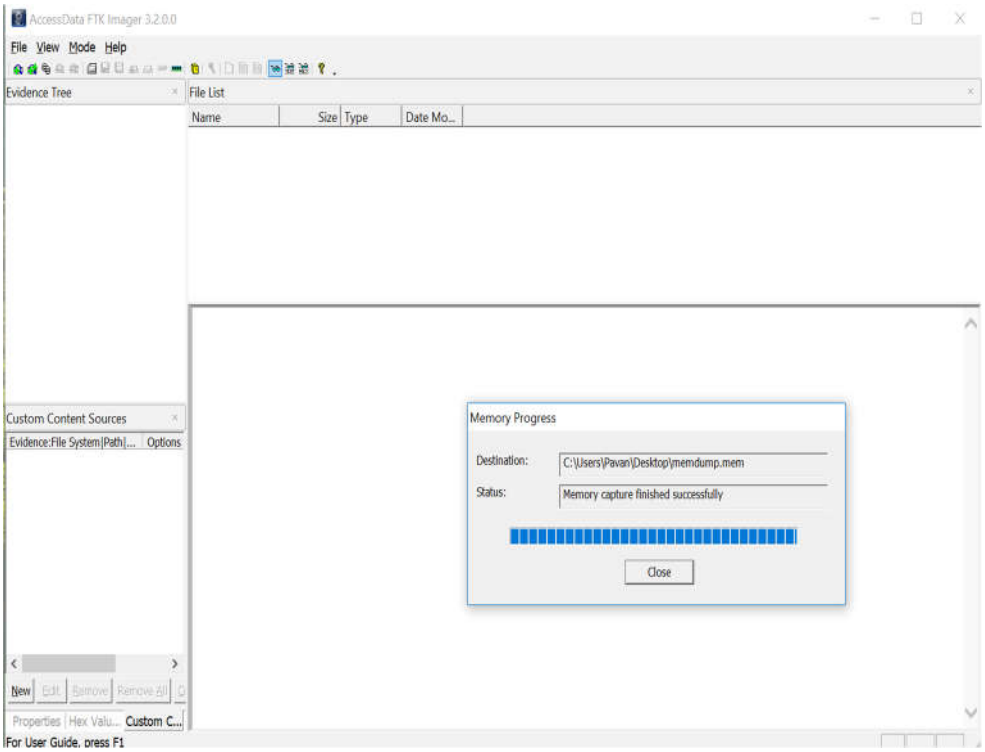
Step 1: Install FTK Imager and click on file and select capture memory



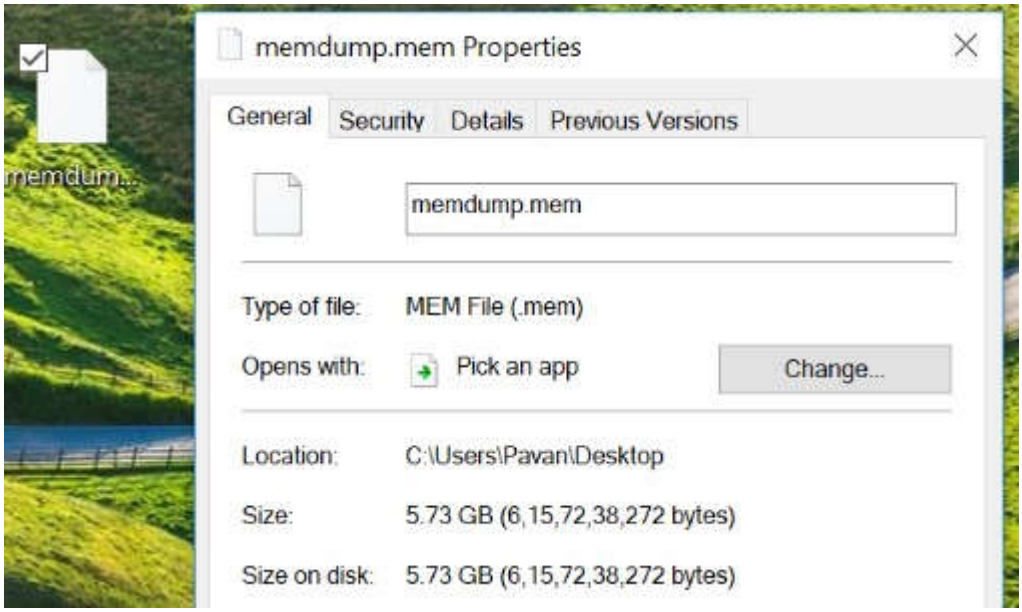
Step 2: Select destination Path for storing the RAM



Step 3: Imaging successful on selected destination drive



Step 4: Captured RAM file.



Exercise 3: Acquire data of a smart phone and extract a report

What you will need?

I. A smart phone
II. A mobile forensic software
III. Data cable

Steps involved in the exercise

1. Use mobile forensic software if available, and installed on desktop
2. Unlock the smart phone and connect it to the system
3. Acquire logical image of the mobile phone

Note: Some mobile forensic software's will ask to enable USB debugging mode and developer options for acquiring the data stored on mobile phones

Exercise 4: Create/generate a hash of a file

What you will need?

I. A free hash calculating software
II. A *.txt or *.doc file

Steps involved in the exercise

1. Open any of the free/open source hash calculating software e.g. HashCalc, Hashtab HashTool
2. Open a word/txt file and write "this is a test file" & generate the hash of the file selected
3. Write down the hash value or take the screen shot of the hash generated.
4. Open the same word/txt file and change it is "This is a test file"
5. Generate the hash of the new file
6. Compare both the hashes.

Exercise 5: Extract metadata of a Picture

What you will need?

I. A geo-tag enabled picture from a smart phone
II. Windows 7/8/10 OS, PhotoME, Exif viewers

Steps involved in the exercise

1. Right click on the image to see the metadata of an image on desktops having windows 7/8/10 OS.
2. Open the image with free Exif viewers

Exercise 6: Get details of IP and MAC address, date & time of a system

Steps involved in this exercise

1. For windows based system type *ipconfig/all* in command prompt and take the screenshot
2. For windows based system type *date/t & time/t* in command prompt and take the screen shot

- For Linux based system *ifconfig –a* command can be used to view IP & MAC address and *date* command can be used to display date and time of the machine.

Note: Alternatively *getmac* on windows and *ip link* can be used to display mac address of the machine

Exercise 7: create an image of pen dive or hard disk and perform a key word search on the created image e.g. hack, password, porn, fake, murder etc., using disk analysis software.

Exercise 8: Extract the windows registry files from the OS and also, extract details of the devices attached through USB on the machine.

Annexure 1

(_____Police Station

Crime No. u/s _____)

OR

(Certifying Organisation Letter Head)

CERTIFICATE UNDER SECTION 65(B) OF THE INDIAN EVIDENCE ACT, 1872

This is to certify that:

1. Printouts of all the documents/Data in CD/DVD/Pen drive were produced by the computer during the period over which the computer was used regularly to store and process information for the purposes of this activity.
2. That these outputs were produced by the computer of _____ (HP/DELL/ACER/etc.) company, which has been allotted to me by _____ (organization/department) for official/business use.
3. This computer system is installed in _____ (place where the system is installed).
4. This computer system is used regularly to store or process information for the purpose of _____ (business/official use).
5. Being a _____ (computer user's designation/profile) I have got the lawful control over the use of this computer system.
6. During the said period, information contained in the electronic record derived was regularly fed into the computer in the ordinary course of the said activities.
7. Throughout the material part of the said period, the computer was operating properly.
8. The information contained in this electronic record reproduced or is derived from such information fed into the computer in the ordinary course of the said activities.

It has been stated to the best of my knowledge and belief.

(_____)

Date: (certifying person sign, name & designation)

Place:

Annexure 2

A sample copy of certificate u/s. 65B of IEA issued by MSP- Aircel for authenticating Call Data Records (CDR)

AIRCEL

CERTIFICATE

(U/s 65B (4) (C) of the Indian Evidence Act 1872)

It is to certify that the CDR's produced of the Mobile Number 9942[redacted]2 for the search period from [redacted]5 to 1[redacted], has been generated from company's computer system contains pages from 1 to 61 and its contents conform to the records and are true to the best of my knowledge. Further certified that the conditions as laid down in section 65B(2)(a) to 65B(2)(d) of Indian Evidence Act 1872 regarding the admissibility of computer output in relation to the information and Computers & servers in question are fully satisfied in all respects

(a) The server output containing the information was produced by the computer during the period over which the same was regularly used to store or processing of CDRs regularly and the undersigned having lawful control over the said computer/Server Application.

(b) During the said period, The information of the kind contained in electronic record or of the kind from which the information is derived was regularly fed into the computer in the ordinary course of the said activities

(c) Throughout the material part of the said period, the computer was operating properly or, if not, then in respect of any period in which it was not operating or was out of operation during that part of the period, was not such as to affect the electronic record or the accuracy of its contents; and

(d) The information contained in the record reproduces or derived from such information fed into the computer in the ordinary course of the said activities.

Thanking you,

Yours sincerely,
For **Aircel Limited**

AIRCEL LIMITED CHENNAI 600 002

R.Arunagiri
Sr.Executive - Regulatory & Nodal

Aircel Limited
Registered Office: 5th Floor, Spencer Plaza, 769, Anna Salai, Chennai (TN) 600002
Corporate Identity Number: U32201TN1994PLC029608, Tel No: +91 44 28490849, Fax No: +91 44 28496769 / 42280155
Email: corporate.al@aircel.co.in Website: www.aircel.com

Annexure 3

List of Nodal officers of Service Providers:

Nodal Service Providers List				
S no.	**Name of the Service provider**	**Area Of Operation**	**Name of the Nodal Officer**	**Email ID/ Reporting Link**
1	Facebook	All India	Vikram	https://www.facebook.com/records/login/
2	Instagram	All India		Same as above
3	Pinterest	All India		https://help.pinterest.com/en/law-enforcement
4	Twitter	All India		https://legalrequests.twitter.com/forms/landing_disclaimer lawenforcement@twitter.com
5	Google	All India	Gitanjali	gitanjli@google.com lis-apac@google.com
6	Microsoft	All India		indiacc@microsoft.com
7	Locanto	All India		support@locanto.in
8	GMAIL	All India	Legal Desk	lis-apac@google.com
9	Rediff	All India	LEA Support	customersupport@rediff.co.in legal@rediff.co.in
10	Sify	All India	LEA Support	lea.support@sifycorp.com
11	Skype	All India	Legal Desk	lerm@skype.net
12	Bharat Matrimony	All India		legal@consim.com
13	Ola	All India		cybercrimeescalations@olacabs.com, cccell@olacabs.com
14	Uber	All India		LERT@uber.com
15	Xvideos	All India		content@xvideos.com
16	mobikwik	All India		fraudalerts@mobikwik.com, risk@mobikwik.comrisk@mobikwik.com
17	oxigen	All India		fraud.control@myoxigen.com
18	Paytm One97Communication	All India		cybercell@paytm.com
19	flipkart.com	All India	Murthy	murthy.sn@flipkart.com, escalationdesk@flipkart.com
20	AMAZON	All India		police-inquiries@amazon.in, police-inquiries-India@amazon.in, cs-reply@amazon.in
21	Yahoo	All India	Mr. Robin	robinfe@yahoo-inc.com

Annexure 4

Recommended timetable - Investigation course

Morning Session

Day	9:30 to 10:00	10:00 to 10:45	10:45 to 11:30	Tea Break	11:45 to 12:30	12:30 to 13:15	13:15 to 14:00	Lunch
1	Registration and Inauguration	Overview of Cybercrimes **(Chapter 1)**		Tea Break	Information Gathering Case Study / Scenario Analysis **(Chapter 10)**			Lunch
2		Scene of Crime Management: Pre-Research Preparation & Required Forensic tool kits **(Chapter 8)**		Tea Break	Scene of Crim Management: Search, Seizure & Documentation **(Chapter 8)**			Lunch
3		IP, Websites & Email Investigation **(Chapter 2)**		Tea Break	IP, Websites & Email Investigation case study **(Chapter 2)**	Communication Device (Mobile Phone, Satellite Phone, GPS Device Etc) Based Investigation **(Chapter 4)**		Lunch
4		Social Media Investigation **(Chapter 3)**		Tea Break	Social Media Investigation Case Study **(Chapter 10)**	Crime Against Women & Child	Financial Frauds **(Chapter 6)**	Lunch
5		Cyber Laws **(Chapter 9)**		Tea Break	Investigation Challenges		Simulation & Evaluation Exercises **(Lab Exercises)**	Lunch

Afternoon Session

Day	15:00 to 15:45	15:45 to 16:30	Tea Break	16:45 to 17:30
1	Information Gathering (Case Study Exercise) **(Chapter 10)**	Scene of Crime Management, Inspection, Documentation, Securing SOC **(Chapter 8)**	Tea Break	Scene of Crime Management, inspection, Documentation, Securing SOC **(Chapter 8)**
2	Scene of Crime Management: Simulation Exercises **(Lab Exercises)**		Tea Break	Scene of Crime Management: Group Exercise
3	Communication Device (Mobile Phone, Satellite Phone, GPS Device Etc) Based Investigation **(Chapter 5)**		Tea Break	Communication Device (Mobile Phone, Satellite Phone, GPS Device Etc) Based Investigation **(Chapter 5)**
4	Financial Frauds Case Study **(Chapter 10)**		Tea Break	Investigation Abroad **(Chapter 7)**
5	Simulation & Evaluation Exercises **(Lab Exercises)**		Tea Break	Valediction